Laboratorio di Sistemi e Reti

1. Realizzazione di una VPN: protocolli ISAKMP e IPsec

Classe 5^A - Indirizzo Informatica

Emanuele Bertolero

Istituto Tecnico Industriale “Don Luigi Orione”

Le fasi principali

Nella creazione di una VPN fasi principali sono due:

- Fase 1 - Stabilire un canale sicuro (IKE Phase 1):
  I dispositivi coinvolti nella VPN negoziano i parametri di sicurezza, si autenticano a vicenda e stabiliscono una Security Association (SA) utilizzando il protocollo ISAKMP. Scambiano chiavi crittografiche tramite il gruppo Diffie-Hellman per creare un canale sicuro e affidabile.

- Fase 2 - Proteggere il traffico dei dati (IKE Phase 2):
  Una volta stabilito il canale sicuro si inizia con la negoziazione delle Security Associations per il traffico effettivo tra i dispositivi e si utilizza IPsec (Internet Protocol Security) per proteggere il traffico dei dati tra i dispositivi.

Protocollo ISAKMP

ISAKMP è un protocollo per la gestione di associazioni di sicurezza e chiavi crittografiche nelle reti, e i suoi parametri definiscono le modalità di autenticazione, crittografia, integrità e scambio di chiavi per stabilire comunicazioni sicure tra dispositivi e sono i seguenti:

- Key Distribution Method: specifica il metodo utilizzato per la distribuzione delle chiavi crittografiche durante l'inizializzazione della comunicazione tra due peer

Comando: `crypto <valore> policy 10`

Può valere: "isakmp" o "manual"

Protocollo ISAKMP (2)

- Encryption Algorithm: specifica l'algoritmo di crittografia utilizzato per proteggere i dati scambiati tra due peer ISAKMP

  Comando: `encryption <valore>`

  Può valere: "DES" o "3DES" o "AES"

- Hash Algorithm: specifica l'algoritmo utilizzato per generare un hash dei dati crittografati. Ciò garantisce l'integrità dei dati e la non-ripudiabilità delle transazioni

  Comando: `hash <valore>`

  Può valere: "MD5" o "SHA-1"

Protocollo ISAKMP (3)

- Authentication Method: specifica il metodo utilizzato per autenticare i peer coinvolti nella comunicazione

Comando: `authentication <valore>`

Può valere: "pre-share" o "RSA"

- IKE SA Lifetime: determina la durata massima di una Security Association (SA) stabilita dall'Internet Key Exchange (IKE) dopo la quale l'SA scadrà e sarà necessario negoziare una nuova

Comando: `lifetime <valore>`

Numero intero in secondi

Protocollo ISAKMP (4)

- Key Exchange: indica il metodo utilizzato per gli scambi delle chiavi criptografiche tra i peer, questi metodi consentono ai due host di stabilire un segreto condiviso da usare come chiave simmetrica per la crittografia dei dati

Comando: `group <valore>`

Può valere: "1", "2" o "5"

Il valori fanno riferimento al protocollo Diffie-Hellman e rappresentano la grandezza del primo numero primo predefinito (p) e di una radice primitiva modulo p generata casualmente (g), utilizzati per la generazione delle chiavi.
DH gruppo 1: p=768 bit, g =2
DH gruppo 2: p=1024 bit, g=2.
DH gruppo5: p=2048 bit, g=nuova radice

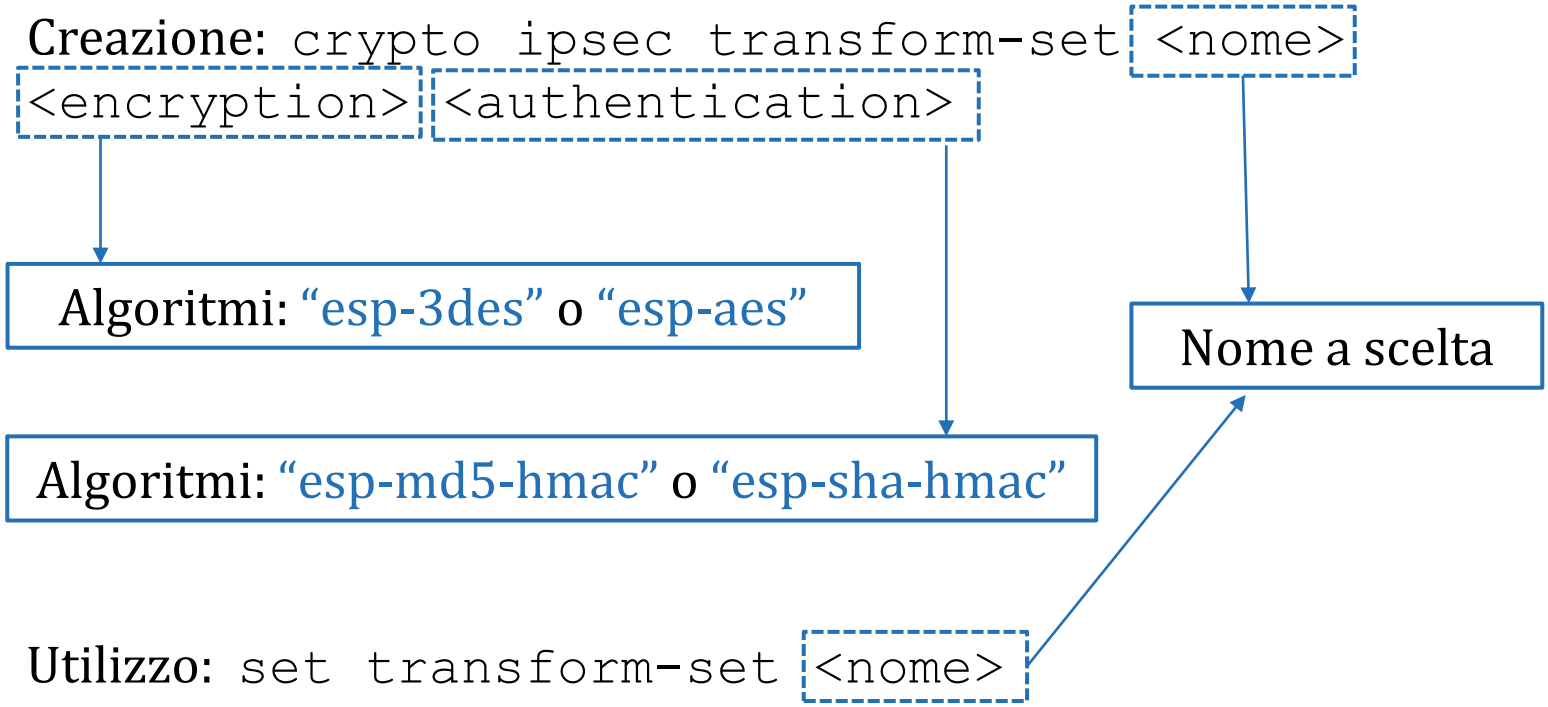
Protocollo IPsec

IPsec viene utilizzato per garantire la sicurezza e l'integrità dei dati trasmessi attraverso la rete. I suoi parametri includono il modo in cui i pacchetti vengono crittografati e autenticati, il tipo di algoritmo di hash utilizzato per proteggere i dati, e la durata delle associazioni che regolano lo scambio delle chiavi e sono i seguenti:

- ESP Transform Encryption: specifica l'algoritmo di cifratura a blocchi utilizzato dall'Encapsulating Security Payload (ESP) per proteggere i dati durante la comunicazione tra due peer IPSEC,
- ESP Transform Authentication: specifica l'algoritmo di autenticazione dei dati utilizzato dall'Encapsulating Security Payload (ESP) per verificare l'integrità dei pacchetti durante la comunicazione tra due peer IPSEC., i valori possibili includono algoritmi HMAC

Protocollo IPsec (2)

- Transform Set Name: specifica l'elenco di trasformazioni crittografiche da applicare ad un pacchetto IP durante la comunicazione tra due peer IPSEC



Protocollo IPsec (3)

- Peer IP Address: si riferisce all'indirizzo IP del peer remoto o della sua interfaccia di rete da cui ci si aspetta di ricevere traffico crittografato. Il valore può essere un indirizzo IPv4 o IPv6, a seconda della versione del protocollo Internet utilizzato.

Comando: `set peer <indirizzo>`

Indirizzo IP

- Traffic to be Encrypted: specifica quali tipi di traffico devono essere protetti dalla crittografia. I valori possibili includono IPv4, IPv6 e protocolli applicativi come TCP e UDP

Comando: `match address <valore>`

Origine-destinazione dei pacchetti

Protocollo IPsec (4)

- SA Establishment: specifica il metodo utilizzato per stabilire le Security Associations tra due peer IPSEC

- Crypto Map Name: specifica il nome identificativo della mappa crittografica che definisce la gestione e l'applicazione delle politiche di sicurezza per una particolare VPN

Comando: `crypto map <nome> <n> <establishment>`

Metodo: "ipsec-isakmp" o "manual" o "pki"

POLO TECNICO PROFESSIONALE INDIRIZZO INDUSTRIALE
SCUOLE DON ORIONE FANO

- ISTITUTO TECNICO INDUSTRIALE
- ISTITUTO PROFESSIONALE INDUSTRIA E ARTIGIANATO
- CENTRO DI FORMAZIONE PROFESSIONALE

Emanuele Bertolero

emanuele.bertolero@donorionefano.edu.it