Laboratorio di RETI di TELECOMUNICAZIONE

Andrea Piroddi

Dipartimento di Ingegneria Scienze e Informatica

VPN-IPSEC - Cenni di Teoria

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

VPN IPSEC – Cenni di Teoria

VPN IPSEC – Cenni di Teoria

1. Cos'è una VPN IPsec?

- Una **VPN (Virtual Private Network)** permette di creare una connessione sicura e criptata tra due reti o dispositivi su una rete pubblica, come Internet.
- **IPsec (Internet Protocol Security)** è un insieme di protocolli che fornisce autenticazione, integrità e crittografia per i pacchetti IP, permettendo la creazione di VPN sicure.

2. Principali Caratteristiche di IPsec:

- **Crittografia**: IPsec cripta i pacchetti dati per garantire la riservatezza del traffico.
- **Integrità**: Utilizza algoritmi di hashing per assicurarsi che i dati non vengano alterati durante la trasmissione.
- **Autenticazione**: Verifica l'identità delle parti coinvolte nella comunicazione.

VPN IPSEC – Cenni di Teoria

3. Modalità di Funzionamento:

- **Transport Mode**: Solo il payload del pacchetto IP è criptato, mantenendo l'intestazione IP originale. Tipicamente usato per la comunicazione host-to-host.

- **Tunnel Mode**: L'intero pacchetto IP, compresa l'intestazione, è criptato. Un nuovo header IP viene aggiunto per instradare il pacchetto. Questa modalità è più comune nelle VPN site-to-site.

VPN IPSEC – Cenni di Teoria

Fasi del Protocollo Ipsec

1. **Fase 1: ISAKMP/IKE (Internet Key Exchange)**

   – È il processo di negoziazione iniziale che stabilisce un canale sicuro tra le due parti.

   – **IKE (Internet Key Exchange)** negozia la crittografia, l'autenticazione e l'integrità utilizzando un protocollo come Diffie-Hellman per lo scambio delle chiavi.

   – In questa fase si crea il **Security Association (SA)**, che è un accordo tra le due parti sui parametri di sicurezza.

VPN IPSEC – Cenni di Teoria

Step della Fase 1:

- **Policy Negotiation**: I router o firewall negoziano i metodi di crittografia e hash da usare.
- **Scambio delle chiavi Diffie-Hellman**: Scambio sicuro delle chiavi per la cifratura.
- **Autenticazione**: Viene verificata l'identità degli endpoint.

Esito: un tunnel sicuro attraverso cui avverrà la fase 2.

VPN IPSEC – Cenni di Teoria

2. Fase 2: Stabilire il Tunnel Ipsec

- In questa fase viene creata una seconda **Security Association (SA)**, che stabilisce il tunnel IPsec per criptare i dati.

- Gli algoritmi di crittografia e autenticazione (come AES e SHA) stabiliti durante la fase 1 vengono applicati ai dati reali.

VPN IPSEC – Cenni di Teoria

Step della Fase 2:

- **Negoziazione delle SA IPsec**: Le parti negoziano i parametri di crittografia per il traffico dati.

- **Creazione del Tunnel IPsec**: Viene creato il tunnel per criptare e trasmettere i dati tra le reti.

VPN IPSEC – Cenni di Teoria

Protocolli Ipsec

AH (Authentication Header):

1. AH fornisce **integrità e autenticazione**, ma non crittografia.
2. L'intestazione di autenticazione garantisce che i dati non siano stati modificati durante il transito, ma i dati rimangono in chiaro.

ESP (Encapsulating Security Payload):

1. ESP fornisce **crittografia, integrità e autenticazione**.
2. Cripta il payload (cioè i dati) per garantire la riservatezza e può anche autenticare i dati.
3. ESP è il protocollo più utilizzato nelle VPN IPsec.

VPN IPSEC – Cenni di Teoria

Vantaggi di una VPN Ipsec

1. **Sicurezza**: IPsec fornisce crittografia avanzata, proteggendo i dati trasmessi su reti non sicure come Internet.

2. **Autenticazione**: Solo dispositivi autorizzati possono stabilire il tunnel VPN.

3. **Integrità dei dati**: I dati non possono essere alterati durante il transito senza essere rilevati.

4. **Flessibilità**: Può essere utilizzato in modalità **site-to-site** (tra reti) o **host-to-host** (tra due dispositivi), e supporta entrambe le modalità **Transport** e **Tunnel**.

VPN IPSEC – Cenni di Teoria

Differenza tra VPN Site-to-Site e VPN Remote Access

1. **Site-to-Site**:
   - Utilizzato per collegare intere reti geograficamente separate.
   - Tutto il traffico tra le reti passa attraverso un tunnel IPsec.
   - Esempio: Collegare la rete dell'ufficio A con quella dell'ufficio B tramite Internet.

2. **Remote Access**:
   - Utilizzato per consentire a singoli utenti remoti di connettersi in modo sicuro a una rete aziendale.
   - Di solito è implementato con client software VPN sui dispositivi remoti.

VPN IPSEC – Cenni di Teoria

Come Funziona il Tunnel IPsec: Esempio Pratico

1. **Creazione del Tunnel**:
   - La connessione viene iniziata da uno dei due endpoint (router, firewall, ecc.).
   - Viene avviata la Fase 1 per stabilire il canale sicuro con IKE.
2. **Trasmissione Dati**:
   1. Una volta creato il tunnel nella Fase 2, i pacchetti IP vengono criptati utilizzando ESP.
   2. I pacchetti vengono inviati attraverso Internet in modalità tunnel, garantendo la sicurezza e la privacy.
3. **Decodifica dei Pacchetti**:
   - All'arrivo, il router o il firewall decifra i pacchetti e li instrada verso la destinazione finale.

Algoritmi di Crittografia Utilizzati da IPsec

1. **Crittografia**:
   - **AES (Advanced Encryption Standard)**: Una delle opzioni più sicure, usata comunemente con chiavi a 128, 192, o 256 bit.
   - **3DES (Triple DES)**: Un metodo di crittografia più vecchio ma ancora utilizzato, che applica DES tre volte su ogni blocco di dati.

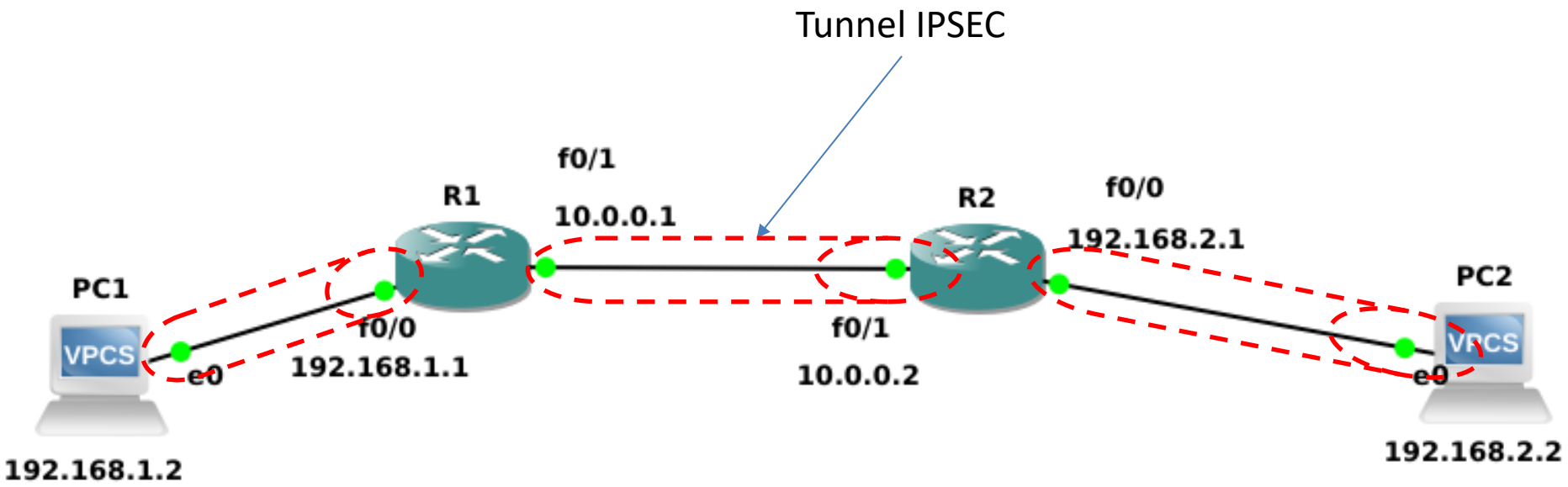
2. **Autenticazione**:
   - **SHA (Secure Hash Algorithm)**: Utilizzato per garantire l'integrità e autenticazione del pacchetto.
   - **MD5 (Message Digest 5)**: Una tecnica di hashing più vecchia ma meno sicura rispetto a SHA.

3. **Scambio delle Chiavi**:
   - **Diffie-Hellman**: Usato per creare una chiave segreta condivisa attraverso una rete non sicura.

VPN IPSEC - Laboratorio

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

VPN IPSEC - Topologia



VPN IPSEC - Topologia

Creazione della Topologia

1. **Aggiungi dispositivi:**
   - Aprite GNS3 e create un nuovo progetto.
   - Aggiungete due router Cisco (R1 e R2) alla topologia.
   - Aggiungete due PC virtuali (PC1 e PC2) per simulare le LAN locali.

2. **Collegamenti:**
   - Collegate **PC1** alla **FastEthernet0/0** di **R1**.
   - Collegate **PC2** alla **FastEthernet0/0** di **R2**.
   - Collegate **FastEthernet0/1** di **R1** a **FastEthernet0/1** di **R2** (questo rappresenta la connessione "Internet").

VPN IPSEC - Topologia

Configurate gli indirizzi IP:

Su R1:

```
conf t
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown

interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
```

VPN IPSEC - Topologia

Configurate gli indirizzi IP:

Su R2:

```
conf t
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
no shutdown

interface FastEthernet0/1
ip address 10.0.0.2 255.255.255.252
no shutdown
exit
```

VPN IPSEC - Topologia

Configurate gli indirizzi IP sui PC:

- **PC1:**

  IP: 192.168.1.2

  Subnet Mask: 255.255.255.0

  Gateway: 192.168.1.1

- **PC2:**

  IP: 192.168.2.2

  Subnet Mask: 255.255.255.0

  Gateway: 192.168.2.1

VPN IPSEC – Configurazione Ipsec VPN

Configurazione di R1 per la VPN IPsec:

```
conf t
! Crea la politica ISAKMP
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
exit

! Imposta la chiave pre-condivisa
crypto isakmp key "password123" address 10.0.0.2

! Crea il set di trasformazione IPsec
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
mode tunnel

! Crea la mappa crittografica
crypto map MYMAP 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set TRANSFORM
match address 100

! Configura l'interfaccia per applicare la mappa
interface FastEthernet0/1
crypto map MYMAP
```

VPN IPSEC – Configurazione Ipsec VPN

Configurazione di R2 per la VPN IPsec:

```
conf t
! Crea la politica ISAKMP
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
exit

! Imposta la chiave pre-condivisa
crypto isakmp key "password123" address 10.0.0.1

! Crea il set di trasformazione IPsec
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
mode tunnel

! Crea la mappa crittografica
crypto map MYMAP 10 ipsec-isakmp
set peer 10.0.0.1
set transform-set TRANSFORM
match address 100

! Configura l'interfaccia per applicare la mappa
interface FastEthernet0/1
crypto map MYMAP
```

VPN IPSEC – Configurazione Ipsec VPN

Configurazione delle ACLs:

- **Su R1:**

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

- **Su R2:**

```
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

VPN IPSEC – Configurazione Ipsec VPN

Verifica delle rotte

Assicuratevi che i router abbiano le corrette rotte statiche o dinamiche per raggiungere le reti coinvolte.

Se i router non conoscono come raggiungere la rete opposta, il traffico non sarà inoltrato correttamente.

Usate il comando `show ip route` su entrambi i router per verificare che abbiano una rotta verso la rete remota.

Se state utilizzando rotte statiche, assicuratevi di aver configurato le rotte correttamente.

Ad esempio:

VPN IPSEC – Configurazione Ipsec VPN

Aggiunta rotta su R1:

```
R1(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
R1(config)#exit
R1#
*Mar  1 00:27:35.535: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 10.0.0.2
```

VPN IPSEC – Configurazione Ipsec VPN

Aggiunta rotta su R2:

```
R2(config-if)#$ 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
R2(config)#exit
R2#show
*Mar  1 00:27:01.027: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

VPN IPSEC – Verifica della Configurazione

Verifica della connettività:

Provate a pingare PC2 da PC1 e viceversa. Usate i seguenti comandi:

```
ping 192.168.2.2  # Da PC1
ping 192.168.1.2  # Da PC2
```

VPN IPSEC – Verifica della Configurazione

Dovreste vedere qualcosa del genere su PC1:

```
PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=51.528 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=41.888 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=41.738 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=40.743 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=32.242 ms

PC1>
```

VPN IPSEC – Verifica della Configurazione

Dovreste vedere qualcosa del genere su PC2:

```
PC2> ping 192.168.1.2

192.168.1.2 icmp_seq=1 timeout
84 bytes from 192.168.1.2 icmp_seq=2 ttl=62 time=45.551 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=41.062 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=41.805 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=39.835 ms

PC2>
```


ALMA MATER STUDIORUM
A.D. 1088


ALMA MATER STUDIORUM
A.D. 1088