Corso di Sicurezza nelle reti di telecomunicazioni
a.a. 2008/2009

Soluzione dei quesiti sulla seconda parte del corso

1) Nell'ipotesi che date tre entità A, B e C:

i) A possieda un certificato digitale X.509 $Cert_A$ (con chiave pubblica PU_A) e relativa chiave privata PK_A;

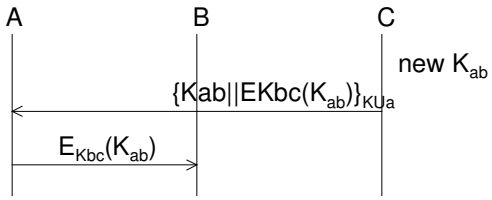
ii) C possieda il certificato di A;

iii) B e C condividano una chiave segreta K_{BC};

iv) B e C non dispongano di alcun canale di comunicazione tra loro.

Si chiede di indicare un possibile schema di comunicazione tramite il quale sia possibile instaurare una associazione sicura tra A e B (K_{AB}).

SOLUZIONE

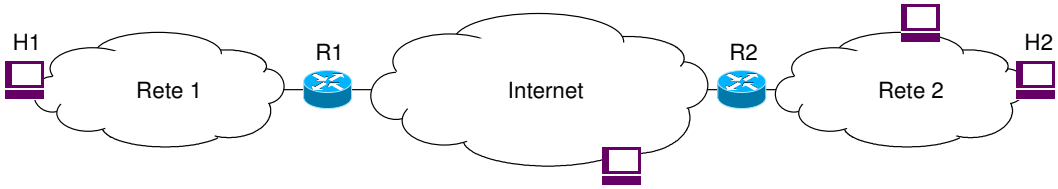


2) Si consideri lo schema di rete rappresentato in figura in cui due sottoreti aziendali sono interconnesse tra loro in VPN tramite rete IP pubblica attraverso IPSec.

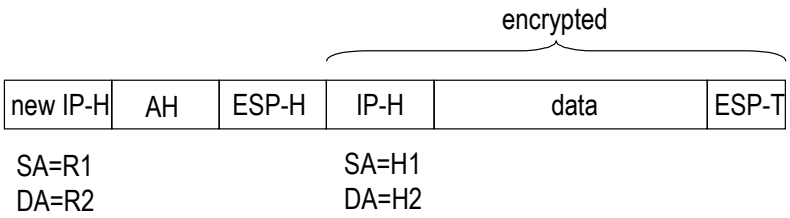
Nell'ipotesi che la VPN sia instaurata tra i router R1 e R2 utilizzando ESP e AH (con AH che protegge anche il contenuto di ESP), e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili (transport/tunnel), si chiede di:

i) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;

ii) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).



SOLUZIONE

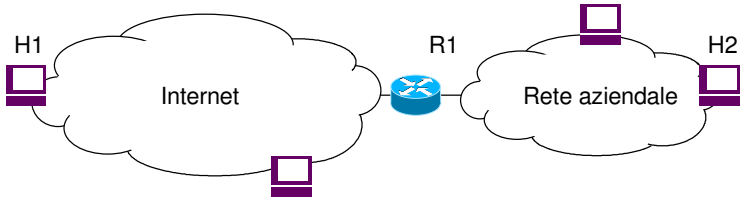


3) Si consideri uno scenario tipo road-warrior in cui un nodo H1 si collega tramite IPSec alla sua rete aziendale e comunichi in modo sicuro con un nodo interno H2, come rappresentato in figura.

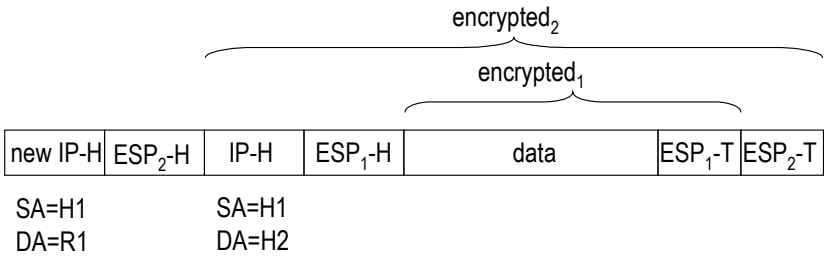
Nell'ipotesi che H1 si colleghi alla sua rete tramite il router R1 in IPSec/ESP, che H1 protegga la sua comunicazione con il nodo H2 tramite IPSec/ESP, e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili, si chiede di:

iii) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;

iv) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).



SOLUZIONE

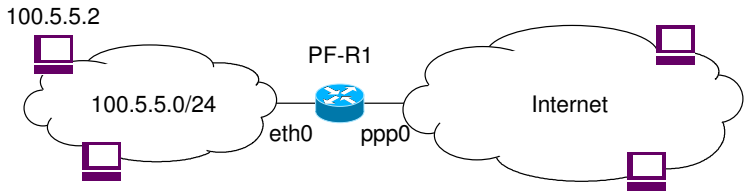


4) Si consideri il seguente schema di rete e si supponga che all'indirizzo 100.5.5.2 sia presente un server web HTTP (porta TCP 80) e un server di posta elettronica SMTP (porta TCP 25); si chiede di configurare la tabella di filtering del router R1 in modo che:

i) sia possibile accedere dall'esterno al server web interno (100.5.5.2),

ii) da tutti in nodi della rete interna sia possible accedere a qualsiasi server web esterno (limitatamente alla porta TCP 80),

iii) sia possibile la comunicazione tra il server SMTP interno de eventuali server SMTP esterni in entrambi i versi (client interno → server esterno porta TCP 25, e server interno porta TCP 25 ← client esterno)



SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	80	state=NEW	ACCEPT
eth0	ppp0	100.5.5.0/24	*	TCP	*	80	state=NEW	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	25	state=NEW	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	*	25	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

Oppure, considerando separatamente le regole anti-spoofing legate alle interfacce:

ppp0	eth0	100.5.5.0/24	*	*	*	*	*	DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
*	*	*	100.5.5.2	TCP	*	80	state=NEW	ACCEPT
*	*	100.5.5.0/24	*	TCP	*	80	state=NEW	ACCEPT
*	*	*	100.5.5.2	TCP	*	25	state=NEW	ACCEPT
*	*	100.5.5.2	*	TCP	*	25	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

Oppure, senza mantenimento dello stato e utilizzando info sui flag TCP:

ppp0	eth0	*	100.5.5.2	TCP	*	80	*	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	80	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
eth0	ppp0	100.5.5.0/24	*	TCP	*	80	*	ACCEPT
ppp0	eth0	*	100.5.5.0/24	TCP	80	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	25	*	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	25	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	*	25	*	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	25	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
*	*	*	*	*	*	*	*	DROP

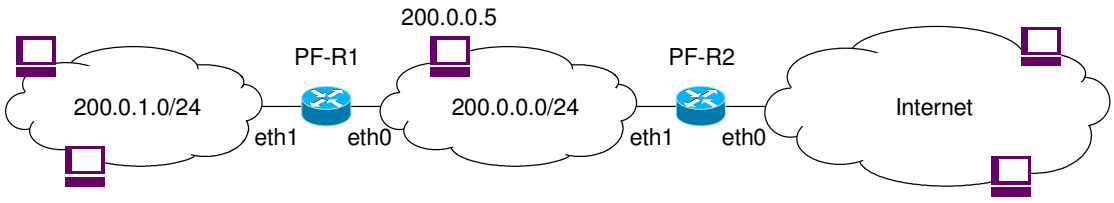
5) Si consideri il seguente schema di rete aziendale composta da una rete interna e da una DMZ separate dal screening router R1 e collegate alla rete esterna (pubblica) tramite il screening router R2.
Si chiede di configurare la tabella di filtraggio (ACL) di R2 in modo che:

a) sia possibile instaurare comunicazioni a livello applicativo client-server (con qualsiasi protocollo di trasporto) da qualsiasi nodo della DMZ verso qualsiasi nodo della rete esterna;

b) sia bloccata qualsiasi comunicazione client/server da rete esterna a DMZ;

c) sia bloccata qualsiasi comunicazione tra rete interna e rete esterna;

d) sia possibile instaurare connessioni TCP da rete esterna al nodo 200.0.0.5, porta 80 (HTTP).



SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
eth1	eth0	200.0.0.0/24	*	*	*	*	state=NEW	ACCEPT
eth0	eth1	*	200.0.0.5	TCP	*	80	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

6) Considerando lo schema di rete dell'esercizio precedente si configuri la tabella di filtraggio (ACL) di R1 in modo che:

e) sia possibile instaurare comunicazioni a livello applicativo client-server (con qualsiasi protocollo di trasporto) da qualsiasi nodo della rete interna (200.0.1.0/24) verso la DMZ;

f) sia bloccata qualsiasi comunicazione client/server da rete DMZ alla rete interna;

g) sia bloccata qualsiasi comunicazione tra rete interna e rete esterna.

SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
eth1	eth0	200.0.1.0/24	200.0.0.0/24	*	*	*	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP