

## **Tecnologies Avançades d'Internet:** Informe pràctica de tunneling **Curs 2016-2017**

NOMS: \_\_\_\_\_

GRUP: \_\_\_\_\_

Heu de desar aquest informe al directori *entregues/tunneling/informe* dilluns 5 de juny a les 23:00h

1. Amb la topologia de xarxa de la pràctica, quina configuració heu hagut d'aplicar al host C1 per poder encaminar paquets de C1 cap a C2 ?
2. Tot just quan acabeu de configurar el túnel, sense haver configurat IPSEC, intercepteu un datagrama generat amb la comanda `ping6`, des de C1, en els punts GW1 (`eth0`) i ISP2 (`eth0`).
  - a) Dibuixeu de forma esquemàtica l'encapsulació d'aquest datagrama en els dos punts d'intercepció.
  - b) Indiqueu les diferències entre les dues encapsulacions. Justifiqueu aquestes diferències.
  - c) Quin és el TTL del datagrama ICMP de echo request en ISP2, `eth0`? Quin era el TTL inicial? Justifica el TTL observat en ISP2 (`eth0`).
  - d) Quin és el Hop Limit (TTL en IPv6) del datagrama anterior quan arriba a C2? Quin era el Hop Limit inicial? Justifica el Hop Limit observat en C2.
3. Volem encaminar un paquet des de C1 cap a C2.  
Indiqueu cada un dels routers pels que passa el datagrama. Per cada router indiqueu si s'està consultant la taula d'encaminament IPV4 o IPV6. Indiqueu la regla de la taula d'encaminament que se satisfà en cada router.

4. Amb la topologia de la pràctica, podríem haver creat
- a) Un túnel directament de C1 cap a C2. Per què?
  - b) Un túnel de C1 cap a GW2. Per què?
5. Tot just quan acabeu de configurar IPSEC, intercepteu un datagrama generat amb la comanda `ping6`, des de C1, en els punts GW1 (`eth0`) i ISP2 (`eth0`).
- a) Dibuixeu de forma esquemàtica l'encapsulació d'aquest datagrama en els dos punts d'intercepció.
  - b) Indiqueu les diferències entre les dues encapsulacions. Justifiqueu aquestes diferències.
6. Feu un `ping6` des de GW1 cap a GW2. El datagrama està xifrat? Per què?

7. Supposeu que teniu la següent configuració de IPSEC en GW1

```
add 10.0.0.1 10.0.3.2 esp 11111 ...
spdadd 10.0.0.1 10.0.3.2 ... out ..
...
```

Suposeu que teniu la següent configuració de IPSEC en GW2

```
add 10.0.0.1 10.0.3.2 esp 22222 ...
```

Genereu un `ping6` de GW1 cap a GW2.

Responen a les següents preguntes i **justifiqueu les vostres respostes**.

- a) Arribarà el datagrama xifrat de GW1 a GW2?
- b) GW2 El podrà desxifrar? Per què? En cas negatiu, com hauria d'estar configurat GW2 per poder desxifrar-lo?

8. Com hauríeu de configurar GW2 per a que pogués respondre a GW1 amb un datagrama també xifrat? Considereu que GW1 ha d'admetre tràfic que li arribi de GW2 tant xifrat com sense xifrar. Indiqueu les comandes que us caldríen en GW1 (GW1.sh) i en GW2 (GW2.sh).

9. Com hauríeu de configurar GW1 i GW2 per a que es complissin les següents condicions:

- GW1 enviés tràfic xifrat a GW2 i que GW2 el pogués desxifrar. GW2 ha d'admetre de GW1 tràfic xifrat i sense xifrar.
- Que GW1 només acceptés tràfic xifrat de GW2.

Indiqueu les comandes que us caldríen en GW1 (GW1.sh) i en GW2 (GW2.sh).

10. L'esquema utilitzat a la pràctica no és còmode. Si tenim  $n$  túnels, hauríem de definir  $2 \cdot n$  claus manualment i configurar-les correctament.

a) Creus que és segura aquesta política de gestió de claus? Perquè?

b) Existeix algún mecanisme que permeti fer l'intercanvi i la gestió de les claus de forma automàtica, entre els extrems dels ordinadors que utilitzen IPSEC?