Tecnologies Avançades d'Internet: Informe pràctica de tunneling
Curs 2016-2017
NOMS: David Cuadrado 1391968, Ramon Guimerà 1400214
GRUP: Tai-C3

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 ?

Al host C1 no s'ha hagut d'aplicar cap configuració, per defecte, tot ho enviava al GW1. Hem hagut de configurar un túnel a GW1 cap a GW2 i viceversa per a encaminar aquests paquets.

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.

El datagrama interceptat a eth0 de GW1 és un datagrama de tipus ipv6.
Mentre's que el datagrama interceptat a eth0 de ISP2 és un datagrama de tipus ipv4 on les seves dades és un datagrama de tipus ipv6.

b) Indiqueu les diferències entre les dues encapsulacions. Justifiqueu aquestes diferències.

El datagrama interceptat a GW1 és un datagrama estàndar de ipv6, mentre's que el de ISP2 és de tipus ipv4, no només són diferents entre si aquests datagrames a nivells de headers i opcions, sinó que el segon, incorpora al primer dins de les seves dades.

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).

El TTL és de 63. El TTl inicial era de 64, a on es resta 1 en el ISP1.

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.

Arriba amb Hop Limit = 62. El Hop Limit inicial era de 64. Es resta 1 a cada gateway per on passa el datagrama.

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.

Quan encaminem el datagrama, a GW1 mirarà la taula IPv6 i encapsularà el datagrama, ja que coincideix amb la norma del router del túnel (2002::/64 dev mitunel). Per a la resta dels ISP encaminaran el datagrama cap al següent ISP, observant la taula IPv4. L'últim ISP (ISP número 3, encaminarà el datagrama cap a GW2. Aquest, el desencapsularà i observarà que és de versió 6, per lo que mirarà la taula IPv6 i enviarà el datagrama al C2.

4. Amb la topologia de la pràctica, podríem haver creat
a) Un túnel directament de C1 cap a C2. Per què?

Si, si haguéssim encapsulat el datagrama en el mateix C1 i C2 i després s'hagués enviat un datagrama IPv6 cap a GWx i rerement encapsulat en IPv4 per a poder ser enviat per la xarxa.

b) Un túnel de C1 cap a GW2. Per què?

Si, hauriem d'haver seguit el mateix procediment que l'anterior descrit però per GW2, tenint en compte, que el datagrama IPv6 es poden utilitzar adreces de versió 4.

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.

En GW1 eth0, és un datagrama de versió 6 amb les dades xifrades i les adreces respectives autenticades.
En ISP2 eth0, el datagrama és, com s'ha dit en respostes anteriors, de versió 4, on dins té el datagrama de versió 6 xifrat i amb la capçalera d'autenticació.

b) Indiqueu les diferències entre les dues encapsulacions. Justifiqueu aquestes diferències.

En GW1 eth0, l'encapsulació és de seguretat i autenticació tot en versió 6, mentre's que en ISP2 eth0, l'encapsulació és a més a més, sobre IPv4.

6. Feu un ping6 des de GW1 cap a GW2. El datagrama està xifrat? Per què?

Si, el datagrama està xifrat, ja que les polítiques definides són per a rangs de xarxa i no per hosts específics. Per lo que tota comunicació entre GW1 i GW2 ha d'estar xifrada.

7. Suposeu 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.
Responeu a les següents preguntes i justifiqueu les vostres respostes.

a) Arribarà el datagrama xifrat de GW1 a GW2?

Si, ja que tant les associacions com les polítiques definides són les correctes a portar a terme per a xifrar de GW1 a GW2.

b) GW2 El podrà desxifrar? Per què? En cas negatiu, com hauria d'estar configurat GW2 per poder desxifrar-lo?

No, ja que, segons l'enunciat, s'enten que GW2 no té la política per a indicar que s'ha de desxifrar.
A GW2 s'hauria d'afegir la següent SP:
spdadd 10.0.0.1/24 10.0.3.2/24 any -P in ipsec esp/transport//require;

8. Com hauríeu de configurar GW2 per a que pogués respondre a GW1 amb un datagrama també xifrat?

A GW2 hauriem d'afegir les següents normes:
add 10.0.3.2 10.0.0.1 esp 15702 -E 3des-cbc "123456789012123456789012";
spdadd 10.0.3.2/24 10.0.0.1/24 any -P out ipsec esp/transport//require;

9. Com hauríeu de configurar GW1 i GW2 per a que es complíssin les següents condicions:
1) GW1 enviés tràfic xifrat a GW2 i que GW2 el pogués desxifrar. GW2 ha d'admetre de GW1 tràfic xifrat i sense xifrar.
A afegir en GW1 i GW2:
add 10.0.0.1 10.0.3.2 esp 15701 -E 3des-cbc "123456789012123456789012";

A afegir en GW1;
spdadd 10.0.0.1/24 10.0.3.2/24 any -P out ipsec esp/transport//require;

2) Que GW1 només acceptés tràfic xifrat de GW2.
A afegir en GW1 i GW2 per a poder xifrar i desxifrar:
add 10.0.3.2 10.0.0.1 esp 15702 -E 3des-cbc "123456789012123456789012";

A afegir en GW1 per a només acceptat tràfic xifrat:
spdadd 10.0.3.2/24 10.0.0.1/24 any -P in ipsec esp/transport//require;

A afegir en GW2 per a xifrar el trànsit:
spdadd 10.0.3.2/24 10.0.0.1/24 any -P out ipsec esp/transport//require;

10. L'esquema utilitzat a la pràctica no és còmode. Si tenim n túnels, hauríem de definir 2*n claus manualment i configurar-les correctament.
a) Creus que és segura aquesta política de gestió de claus? Perquè?

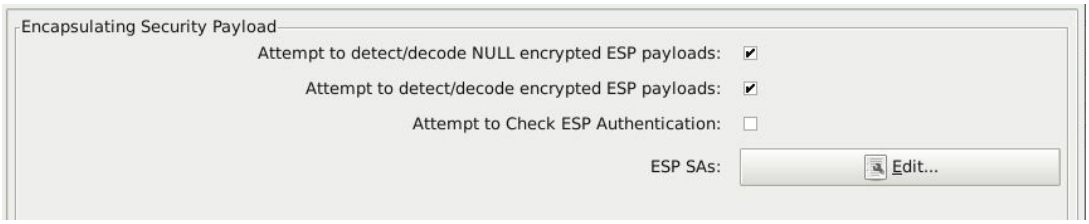
No, ja que és un excés de claus i per a obtenir-les, si no és físicament, no es troba una forma segura.

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?

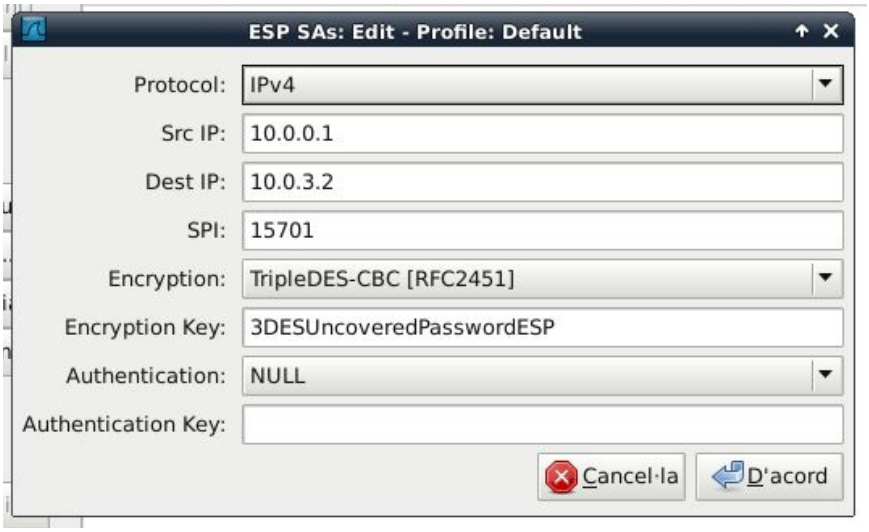
Si, si l'intercanvi de claus es fa a través de Diffie-Hellman o encriptant i signant les claus en RSA.

Opcional:
S'adjunten les captures de pantalles especificades per a la realització de l'opcional de desxifrar un datagrama interceptat xifrat amb ESP.

S'activen les opcions següents pel desxifrat del datagrama:



Rerament, es defineix la SA següent:



El password s'ha obtingut de l'enunciat, passant d'hexadecimal a ASCII.

El missatge contingut en el datagrama era el següent:
"I have something important to talk to you, but can't really write it here since I don't trust the key management policy here…"