ip-xfrm

transform configuration

xfrm est un framework ip pour transformer les paquets (tel que le chiffrement de leur payloads). Ce framework est utilisé pour implémenter la suite de protocole IPsec (avec l'objet state opérant dans la base d'association de sécurité, et l'objet policy opérant dans la base de stratégie de sécurité). Il est également utilisé pour le protocole de compression de payloads et les fonctionnalités IPv6 mobile.

monitor Monitor l'état des objets xfrm

state gére les états dans xfrm

add Ajoute un nouvel état dans xfrm

update Met à jours un état existant dans xfrm

allocspi Alloue une valeur SPI

delete Suppime un état existant dans xfrm

get Récupère un état dans xfrm

deleteall supprime tous les états dans xfrm

list Affiche la liste des états dans xfrm

flush vide tous les état dans xfrm

count compte tous les états existant dans xfrm

ID est spécifié par l'addresse source, l'adresse de destination, le protocole de transformation XFRM-PROTO, et/ou SPI (Security Parameter Index).

XFRM-PROTO Spécifie le protocole de transformation : IPsec Encapsulating Security (esp), IPsec Authentication Header (ah), IP payload Compresion (comp), Mobile IPv6 Type 2 Routing Header (route2), ou Mobile IPv6 Home Address Option (hao)

ALGO-LIST Contient un ou plusieurs algorithmes à utiliser. Chaque algorithme ALGO est spécifié par :

- Le type d'algorithme : encryption (enc), authentication (auth ou auth-trunc), authenticated encryption with associated data (aead), or compression (comp)
- Le nom de l'algorithme ALGO-NAME
- (excepté pour comp) : le clé matérielle (ALGO-KEYMAT), qui peut inclure une clé et un salt ou une aucune valeur.
- (aead uniquement) : la longueur Integrity Check Value ALGO-ICV-LEN en bits.

les algorithmes de chiffrement incluent : ecb(cipher_null), cbc(des), cbc(des3_ede), cbc(cast5), cbc(blowfish), cbc(aes), cbc(serpent), cbc(camellia), cbc(twofish), et rfc3686(ctr(aes)).

Les algorithmes d'authentification inculent : digest_null, hmac(md5), hmac(sha1), hmac(sha256), hmac(sha384), hmac(sha512), hmac(rmd610), et xcbc(aes).

Le chiffrement authentifié avec algorithme de données associée (AEAD) incluent : rfc4106(gcm(aes)), rfc4309(ccm(aes)), et rfc4543(gcm(aes)).

Les algorithmes de compression incluent deflate, lzs et lzjh.

MODE Spécifie un mode d'opérations pour le protocole de transformation. les modes IPsec et IP Payload Compression sont transport, tunnel, et pour IPsec ESP beet (Bound End-to-End Tunnel). les modes Mobile IPv6 sont route optimiszation (ro) et bound trigger (in_trigger).

FLAG-LIST Contient un ou plusieurs flags optionnels suivants : noecn, decap-dscp, nopmtudisc, wildrecv, icmp, af-unspec ou align4

SELECTOR Sélectionne le trafic qui sera contrôlé par la stratégie, basée sur l'adresse source, l'adresse de destination, le périphérique réseau, et/ou UPSPEC.

UPSPEC Sélection le trafic par protocole. Pour tcp, udp, sctp ou dccp, le port source et de destination peut optionnellement être spécifié. Pour les protocoles icmp, ipv6-icmp, ou mobility-headers, le type et le code peuvent optionnellement être spécifiés. Pour le protocole gre, la clé peut optionnellement être spécifié. D'autre protocoles peuvent être sélectionnés par nom ou nombre PROTO.

LIMIT-LIST Définis les limites en secondes, octets, ou nombres de paquets.

ENCAP Encapsule les paquets avec le protocole espinudp, espinudp-nonike, en utilisant le port source SPORT, le port de destination DPORT, et l'adresse originel OADDR.

policy Gère les stratégies dans xfrm

add Ajoute une nouvelle stratégie

update Met à jour une stratégie existante

delete Supprime une stratégie existante

get Récupère une stratégie existante

deleteall Supprime toutes les stratégies xfrm

list Affiche toutes les stratégies xfrm existant

flush Vide les stratégies

count Compte les stratégies existantes

SELECTOR Sélectionne le trafic qui sera contrôlé par la stratégie, basée sur l'adresse sources, l'adresse de destination, le périphérique réseaux, et/ou UPSPEC.

UPSPEC Sélectionne le trafic par protocole. Pour tcp, udp, sctp, ou dccp, le port source et de destination peuvent être optionnellement spécifiés. Pour les protocoles icmp, ipv6-icmp, ou mobility-header, le type et le code peuvent être optionnellement spécifiés. Pour le protocole gre, la clé peut optionnellement être spécifié. D'autres protocoles peuvent être spécifiés par nom ou numéro PROTO.

DIR Sélectionne la direction de la stratégie : in, out ou fwd

CTX Définis le contexte de sécurité

PTYPE Peut être main (défaut) ou sub

ACTION Peut être allow (défaut) ou block

PRIORITY Nombre (défaut : 0)

FLAG-LIST Contient un ou plusieurs flags optionnels : local ou icmp

LIMIT-LIST Définis les limites en secondes, octets, ou nombre de paquets

TMPL-LIST Liste template spécifiée en utilisant ID, MODE, REQID, et/ou LEVEL

ID Spécifié par l'adresse source, l'adresse de destination, le protocole de transformation XFRM-PROTO, et/ou SPI.

XFRM-PROTO Spécifie le protocole de transformation : IPsec Encapsulating Security (esp), IPsec Authentication Header (ah), IP payload Compresion (comp), Mobile IPv6 Type 2 Routing Header (route2), ou Mobile IPv6 Home Address Option (hao)

MODE Spécifie un mode d'opérations pour le protocole de transformation. les modes IPsec et IP Payload Compression sont transport, tunnel, et pour IPsec ESP beet (Bound End-to-End Tunnel). les modes Mobile IPv6 sont route optimiszation (ro) et bound trigger (in_trigger).

LEVEL Peut être required (défaut) ou use.