ipsec

Original file

Краткий план

проверки работоспособности IPSec политики

и

поиска проблем

для прошивок на базе лицензированной NETSHe OS

Для проверки работоспособности и поиска проблем следует выполнить последовательность шагов

Убедиться, что политика загружена

Например, политика gost-ipsec

swanctl —list-conns

pass-mcast: IKEv1/2, no reauthentication, rekeying every 14400s

local: %any

remote: 127.0.0.1

local unspecified authentication:

remote unspecified authentication:

pass-mcast: PASS, no rekeying

local: 0.0.0.0/0

remote: 224.0.0.0/4

gost-ipsec: IKEv2, reauthentication every 28800s, rekeying every 86400s, dpd delay 15s

local: 192.168.25.182

remote: 192.168.25.49

local pre-shared key authentication:

id: 192.168.25.182

remote pre-shared key authentication:

id: 192.168.25.49

gost-ipsec: TUNNEL, rekeying every 86400s, dpd action is restart

local: 192.168.58.0/24

remote: 192.168.59.0/24

Убедиться, что для политки есть SA записи

swanctl —list-sas

gost-ipsec: #1, ESTABLISHED, IKEv2, e947e9f4292464b7_i 28fb87626307809a_r*

local '192.168.25.182' @ 192.168.25.182[500]

remote '192.168.25.49' @ 192.168.25.49[500]

AES_CBC-128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

established 159s ago, rekeying in 79793s, reauth in 28548s

gost-ipsec: #2, reqid 1, INSTALLED, TUNNEL, ESP:3DES_CBC/HMAC_MD5_96

installed 159s ago, rekeying in 77772s, expires in 94881s

in ca249833, 13356 bytes, 159 packets, 0s ago

out c50c4def, 13356 bytes, 159 packets, 0s ago

local 192.168.58.0/24

remote 192.168.59.0/24

В выводе могут/должны быть сведения о числе прошедших пакетов и сумме байт.

Посмотреть вывод ipsec statusall

Status of IKE charon daemon (weakSwan 5.8.2, Linux 4.19.82, x86_64):

uptime: 4 minutes, since Feb 07 17:26:24 2020

worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4

loaded plugins: charon random nonce constraints pubkey pkcs1 pkcs7 pkcs12 af-alg gmp attr kernel-netlink resolve socket-default farp stroke vici updown addrblock

Listening IP addresses:

192.168.25.182

192.168.58.1

Connections:

pass-mcast: %any...127.0.0.1 IKEv1/2

pass-mcast: local: uses any authentication

pass-mcast: remote: uses any authentication

pass-mcast: child: 0.0.0.0/0 === 224.0.0.0/4 PASS

gost-ipsec: 192.168.25.182...192.168.25.49 IKEv2, dpddelay=15s

gost-ipsec: local: [192.168.25.182] uses pre-shared key authentication

gost-ipsec: remote: [192.168.25.49] uses pre-shared key authentication

gost-ipsec: child: 192.168.58.0/24 === 192.168.59.0/24 TUNNEL, dpdaction=restart

Shunted Connections:

pass-mcast: 0.0.0.0/0 === 224.0.0.0/4 PASS

Routed Connections:

gost-ipsec{1}: ROUTED, TUNNEL, reqid 1

gost-ipsec{1}: 192.168.58.0/24 === 192.168.59.0/24

Security Associations (1 up, 0 connecting):

gost-ipsec[1]: ESTABLISHED 3 minutes ago, 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

gost-ipsec[1]: IKEv2 SPIs: e947e9f4292464b7_i 28fb87626307809a_r*, rekeying in 22 hours, pre-shared key reauthentication in 7 hours

gost-ipsec[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

gost-ipsec{2}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca249833_i c50c4def_o

gost-ipsec{2}: 3DES_CBC/HMAC_MD5_96, 20076 bytes_i (239 pkts, 1s ago), 20076 bytes_o (239 pkts, 1s ago), rekeying in 21 hours

gost-ipsec{2}: 192.168.58.0/24 === 192.168.59.0/24

ESTABLISHED в выводе означает, что фаза 1 закончилась успешно.

INSTALLED в выводе означает, что фаза 2 закончилась успешно. Присутствуют счетчики пакетов и байт.

Примеры логов службы IPSec и определение проблемы на основе вывода

Для вывода логов можно использовать команду /opt/stasoft/bin/ipsec-log.sh [x] или

ipsec stroke loglevel any 4

swanctl –log

1. Не совпадают proposals для фазы 1

06[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (418 bytes)

disconnecting...

06[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) V]

06[IKE] received strongSwan vendor ID

06[IKE] 192.168.25.49 is initiating an IKE_SA

06[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

06[CFG] configured proposals: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_768

06[IKE] received proposals unacceptable

06[ENC] generating IKE_SA_INIT response 0 [N(NO_PROP)]

06[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (36 bytes)

2. Не совпадают парольные фразы

11[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (418 bytes)

11[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) V]

11[IKE] received strongSwan vendor ID

11[IKE] 192.168.25.49 is initiating an IKE_SA

11[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

11[CFG] configured proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

11[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

11[ENC] generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) V]

11[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (430 bytes)

06[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (268 bytes)

06[ENC] parsed IKE_AUTH request 1 [IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)]

06[CFG] looking for peer configs matching 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

06[CFG] selected peer config 'gost-ipsec'

06[IKE] tried 1 shared key for '192.168.25.182' - '192.168.25.49', but MAC mismatched

disconnecting...

06[ENC] generating IKE_AUTH response 1 [N(AUTH_FAILED)]

06[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (76 bytes)

3. Не совпадают proposals для фазы 2

15[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (418 bytes)

15[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) V]

15[IKE] received strongSwan vendor ID

15[IKE] 192.168.25.49 is initiating an IKE_SA

15[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

15[CFG] configured proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

15[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

15[ENC] generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) V]

15[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (430 bytes)

07[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (268 bytes)

07[ENC] parsed IKE_AUTH request 1 [IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)]

07[CFG] looking for peer configs matching 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

07[CFG] selected peer config 'gost-ipsec'

07[IKE] authentication of '192.168.25.49' with pre-shared key successful

07[IKE] authentication of '192.168.25.182' (myself) with pre-shared key

07[IKE] destroying duplicate IKE_SA for peer '192.168.25.49', received INITIAL_CONTACT

07[IKE] IKE_SA gost-ipsec[2] established between 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

disconnecting...

07[IKE] scheduling rekeying in 80140s

07[IKE] scheduling reauthentication in 25528s

07[IKE] maximum IKE_SA lifetime 34168s

07[CFG] received proposals: ESP:3DES_CBC/HMAC_MD5_96/NO_EXT_SEQ

07[CFG] configured proposals: ESP:3DES_CBC/HMAC_SHA1_96/MODP_768/NO_EXT_SEQ

07[IKE] no acceptable proposal found

07[IKE] failed to establish CHILD_SA, keeping IKE_SA

07[ENC] generating IKE_AUTH response 1 [IDr AUTH N(AUTH_LFT) N(NO_PROP)]

07[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (124 bytes)

08[IKE] sending DPD request

08[ENC] generating INFORMATIONAL request 0 [ ]

08[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (76 bytes)

05[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (76 bytes)

05[ENC] parsed INFORMATIONAL response 0 [ ]

4. Все совпадает. Туннель создан

13[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (418 bytes)

13[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) V]

13[IKE] received strongSwan vendor ID

13[IKE] 192.168.25.49 is initiating an IKE_SA

13[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

13[CFG] configured proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

13[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536

13[ENC] generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) V]

13[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (430 bytes)

07[NET] received packet: from 192.168.25.49[500] to 192.168.25.182[500] (268 bytes)

07[ENC] parsed IKE_AUTH request 1 [IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)]

07[CFG] looking for peer configs matching 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

07[CFG] selected peer config 'gost-ipsec'

07[IKE] authentication of '192.168.25.49' with pre-shared key successful

disconnecting...

07[IKE] authentication of '192.168.25.182' (myself) with pre-shared key

07[IKE] IKE_SA gost-ipsec[1] established between 192.168.25.182[192.168.25.182]...192.168.25.49[192.168.25.49]

07[IKE] scheduling rekeying in 85745s

07[IKE] scheduling reauthentication in 20238s

07[IKE] maximum IKE_SA lifetime 28878s

07[CFG] received proposals: ESP:3DES_CBC/HMAC_MD5_96/NO_EXT_SEQ

07[CFG] configured proposals: ESP:3DES_CBC/HMAC_MD5_96/MODP_768/NO_EXT_SEQ

07[CFG] selected proposal: ESP:3DES_CBC/HMAC_MD5_96/NO_EXT_SEQ

07[KNL] using encryption algorithm 3DES_CBC with key size 192

07[KNL] using encryption algorithm des3_ede

07[KNL] using encryption algorithm 3DES_CBC with key size 192

07[KNL] using encryption algorithm des3_ede

07[IKE] CHILD_SA gost-ipsec{2} established with SPIs cea50306_i c1be0866_o and TS 192.168.58.0/24 === 192.168.59.0/24

07[ENC] generating IKE_AUTH response 1 [IDr AUTH SA TSi TSr N(AUTH_LFT)]

07[NET] sending packet: from 192.168.25.182[500] to 192.168.25.49[500] (204 bytes)