Le tunnel IPSec site à site s'effondre à chaque modification apportée au modèle de périphérique

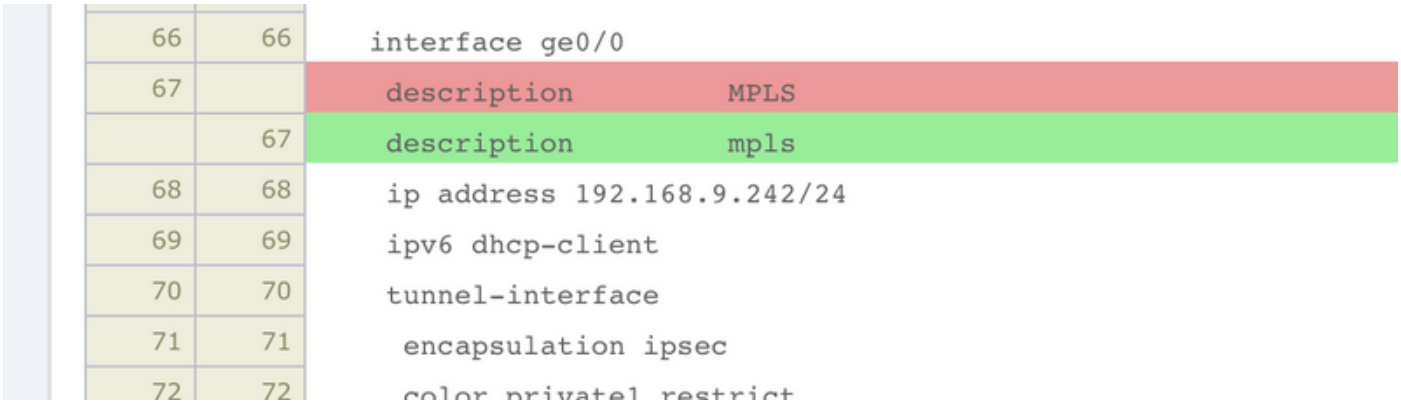
Contenu

Introduction

Ce document décrit le problème typique qui se produit lorsque des tunnels IPSec basés sur l'échange de clés Internet (IKE) de site à site (ou aussi communément appelé LAN-to-LAN) basculent sur chaque mise à jour de modèle de périphérique dans un contrôleur vManage, explique les causes premières et fournit une solution au problème.

Problème

Le tunnel IPSec basé sur IKE s'effondre à chaque fois que le modèle de périphérique est mis à jour sur vManage. Les modifications ne peuvent pas être associées au tunnel IPSec site à site basé sur IKE, mais elles provoquent le blocage du tunnel. Le problème peut être encore plus grave si, par exemple, l'appairage eBGP s'exécute sur un tunnel IPSec. En raison du suivi de l'interface eBGP, le voisin fait également volte-face et, par conséquent, toutes les routes sont retirées puis réinstallées. Cela entraîne une interruption du trafic à son tour. Par exemple, il s'agit de la seule modification apportée au modèle, confirmée par config-preview, comme l'illustre l'image.



Voici à quoi ça ressemble dans les journaux :

```
tail /var/log/vsyslog -f -n 0
local7.info: Nov 26 15:21:08 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-ftmd-6-INFO-
1400002: Notification: 11/26/2019 14:21:8 fib-update severity-level:minor host-name:"BRU-SDW-
V5K-01" system-ip:10.10.10.242 vpn-id:1 address-family-type:ipv4 fib-last-update-time:2019-11-
26T15:18:09+00:00
local7.info: Nov 26 15:21:13 BRU-SDW-V5K-01 BGP.1[6505]: %ADJCHANGE: neighbor 10.0.0.1 Down
local7.info: Nov 26 15:21:13 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-FTMD-6-INFO-
```

```
1000001: VPN 1 Interface ipsec1 DOWN
local7.info: Nov 26 15:21:13 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:21:13 bgp-peer-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 peer:10.0.0.1 bgp-new-state:idle local-
address:10.0.0.2 local-routerid:10.10.10.242 peer-routerid:192.168.9.1
local7.info: Nov 26 15:21:13 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-ftmd-6-INFO-
1400002: Notification: 11/26/2019 14:21:13 interface-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 if-name:"ipsec1" new-state:down
local7.info: Nov 26 15:21:13 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:21:13 system-commit severity-level:minor host-name:"BRU-
SDW-V5K-01" system-ip:10.10.10.242 user-name:"vmanage-admin"
local7.info: Nov 26 15:21:14 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-FTMD-6-INFO-
1000001: VPN 1 Interface ipsec1 UP. Speed 10 Duplex Full
local7.info: Nov 26 15:21:14 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-ftmd-6-INFO-
1400002: Notification: 11/26/2019 14:21:14 interface-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 if-name:"ipsec1" new-state:up
local7.warn: Nov 26 15:21:18 BRU-SDW-V5K-01 BGP.1[6505]: 10.0.0.1 unrecognized capability code:
70 - ignored
local7.info: Nov 26 15:21:18 BRU-SDW-V5K-01 BGP.1[6505]: %ADJCHANGE: neighbor 10.0.0.1 Up
local7.info: Nov 26 15:21:18 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:21:18 bgp-peer-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 peer:10.0.0.1 bgp-new-state:established
local-address:10.0.0.2 local-routerid:10.10.10.242 peer-routerid:192.168.9.1
```

Comme vous pouvez le voir, le voisin BGP a clignotant. Dans le document **/var/log/messages** vous pouvez voir plus d'informations :

```
auth.info: Nov 26 15:24:38 BRU-SDW-V5K-01 sshd[27423]: Accepted publickey for vmanage-admin from
10.10.10.253 port 40555 ssh2: RSA SHA256:ySiw9uiBxffv6HrO0iwDE3jm05mmO4IQoc+qgzfuyd4
authpriv.info: Nov 26 15:24:38 BRU-SDW-V5K-01 sshd[27423]: pam_unix(sshd:session): session
opened for user vmanage-admin by (uid=0)
local1.info: Nov 26 15:24:38 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 assigned
to groups: vmanage-admin,log
local1.info: Nov 26 15:24:38 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 new tcp session for
user "vmanage-admin" from 10.10.10.253
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}get attrs: nc:message-id="1"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-
id="1"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="1"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}get attrs: nc:message-id="2"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-
id="2"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="2"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}get attrs: nc:message-id="3"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-
id="3"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="3"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}get attrs: nc:message-id="4"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-
id="4"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="4"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}lock attrs: nc:message-id="5"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 lock target=candidate
attrs: nc:message-id="5"
```

```
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="5"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}copy-config attrs: nc:message-id="6"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 copy-config
source=running target=candidate attrs: nc:message-id="6"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="6"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}edit-config attrs: nc:message-id="7"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 edit-config
target=candidate attrs: nc:message-id="7"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="7"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}validate attrs: nc:message-id="8"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 validate
source=candidate attrs: nc:message-id="8"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="8"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}validate attrs: nc:message-id="9"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 validate source=inline
attrs: nc:message-id="9"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="9"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}edit-config attrs: nc:message-id="10"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 edit-config
target=candidate attrs: nc:message-id="10"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="10"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}commit attrs: nc:message-id="11"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 commit attrs:
nc:message-id="11"
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 14[CFG] unloaded shared key with id
'ipsec1_1'
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 07[CFG] vici terminate IKE_SA 'ipsec1_1'
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] closing CHILD_SA child_ipsec1_1{8}
with SPIs 00000107_i (6247108 bytes) 12107f74_o (6235990 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] closing CHILD_SA child_ipsec1_1{8}
with SPIs 00000107_i (6247108 bytes) 12107f74_o (6235990 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[KNL] Deleting SAD entry with SPI 00000107
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[KNL] Deleting SAD entry with SPI 12107f74
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] sending DELETE for ESP CHILD_SA with
SPI 00000107
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[ENC] generating INFORMATIONAL_V1 request
226869087 [ HASH D ]
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (76 bytes)
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] closing CHILD_SA child_ipsec1_1{9}
with SPIs 00000108_i (6247912 bytes) 1286959a_o (6235990 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] closing CHILD_SA child_ipsec1_1{9}
with SPIs 00000108_i (6247912 bytes) 1286959a_o (6235990 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[KNL] Deleting SAD entry with SPI 00000108
local7.info: Nov 26 15:24:39 BRU-SDW-V5K-01 BGP.1[6505]: %ADJCHANGE: neighbor 10.0.0.1 Down
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[KNL] Deleting SAD entry with SPI 1286959a
local7.info: Nov 26 15:24:39 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-FTMD-6-INFO-
1000001: VPN 1 Interface ipsec1 DOWN
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] sending DELETE for ESP CHILD_SA with
SPI 00000108
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[ENC] generating INFORMATIONAL_V1 request
2972009957 [ HASH D ]
```

```
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (76 bytes)
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] deleting IKE_SA ipsec1_1[10] between
192.168.9.242[192.168.9.242]...192.168.9.1[192.168.9.1]
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] deleting IKE_SA ipsec1_1[10] between
192.168.9.242[192.168.9.242]...192.168.9.1[192.168.9.1]
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] sending DELETE for IKE_SA
ipsec1_1[10]
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[ENC] generating INFORMATIONAL_V1 request
956819772 [ HASH D ]
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (92 bytes)
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 begin
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 /viptela-vpn:vpn/vpn-instance{0}/interface{ge0/0}/description set to "mpls"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 /viptela-vpn:vpn/vpn-instance{1}/interface{ipsec1}/ike/authentication-type/pre-
shared-key/pre-shared-secret set to "*****"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 /viptela-system:system/pseudo-confirm-commit set to "300"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 end
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="11"
local7.info: Nov 26 15:24:39 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:24:39 bgp-peer-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 peer:10.0.0.1 bgp-new-state:idle local-
address:10.0.0.2 local-routerid:10.10.10.242 peer-routerid:192.168.9.1
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/vpn}bgp-peer-state-change
local7.info: Nov 26 15:24:39 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-ftmd-6-INFO-
1400002: Notification: 11/26/2019 14:24:39 interface-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 if-name:"ipsec1" new-state:down
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/vpn}interface-state-change
local7.info: Nov 26 15:24:39 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:24:39 system-commit severity-level:minor host-name:"BRU-
SDW-V5K-01" system-ip:10.10.10.242 user-name:"vmanage-admin"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/system}system-commit
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 14[CFG] added vici connection: ipsec1_1
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 14[CFG] loaded IKE shared key with id
'ipsec1_1' for: '192.168.9.242', '192.168.9.1'
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 14[CFG] vici initiate 'child_ipsec1_1'
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 15[IKE] initiating Main Mode IKE_SA
ipsec1_1[11] to 192.168.9.1
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 15[IKE] initiating Main Mode IKE_SA
ipsec1_1[11] to 192.168.9.1
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 15[ENC] generating ID_PROT request 0 [ SA V
V V V V ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 15[NET] sending packet: from
192.168.9.242[500] to 192.168.9.1[500] (180 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 06[NET] received packet: from
192.168.9.1[500] to 192.168.9.242[500] (104 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 06[ENC] parsed ID_PROT response 0 [ SA V ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 06[IKE] received NAT-T (RFC 3947) vendor ID
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 06[ENC] generating ID_PROT request 0 [ KE No
NAT-D NAT-D ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 06[NET] sending packet: from
192.168.9.242[500] to 192.168.9.1[500] (244 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[NET] received packet: from
192.168.9.1[500] to 192.168.9.242[500] (304 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[ENC] parsed ID_PROT response 0 [ KE No V
```

```
V V V NAT-D NAT-D ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[IKE] received Cisco Unity vendor ID
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[IKE] received DPD vendor ID
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[ENC] received unknown vendor ID:
5e:b0:e6:33:27:48:bf:3b:80:a6:a7:d5:cd:37:64:1f
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[IKE] received XAuth vendor ID
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[IKE] faking NAT situation to enforce UDP
encapsulation
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[ENC] generating ID_PROT request 0 [ ID
HASH N(INITIAL_CONTACT) ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 08[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (108 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[NET] received packet: from
192.168.9.1[4500] to 192.168.9.242[4500] (76 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[ENC] parsed ID_PROT response 0 [ ID HASH
]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[IKE] IKE_SA ipsec1_1[11] established
between 192.168.9.242[192.168.9.242]...192.168.9.1[192.168.9.1]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[IKE] IKE_SA ipsec1_1[11] established
between 192.168.9.242[192.168.9.242]...192.168.9.1[192.168.9.1]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[IKE] scheduling rekeying in 13069s
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[IKE] maximum IKE_SA lifetime 14509s
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[ENC] generating QUICK_MODE request
1775307947 [ HASH SA No KE ID ID ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 07[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (316 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[NET] received packet: from
192.168.9.1[4500] to 192.168.9.242[4500] (348 bytes)
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[ENC] parsed QUICK_MODE response
1775307947 [ HASH SA No KE ID ID N((24576)) ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[KNL] add SAD entry with SPI 00000109
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[KNL] add SAD entry with SPI d8c172fc
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[IKE] CHILD_SA child_ipsec1_1{10}
established with SPIs 00000109_i d8c172fc_o and TS 0.0.0.0/0 === 0.0.0.0/0
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[IKE] CHILD_SA child_ipsec1_1{10}
established with SPIs 00000109_i d8c172fc_o and TS 0.0.0.0/0 === 0.0.0.0/0
local7.info: Nov 26 15:24:40 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-FTMD-6-INFO-
1000001: VPN 1 Interface ipsec1 UP. Speed 10 Duplex Full
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[ENC] generating QUICK_MODE request
1775307947 [ HASH ]
daemon.info: Nov 26 15:24:40 BRU-SDW-V5K-01 charon: 11[NET] sending packet: from
192.168.9.242[4500] to 192.168.9.1[4500] (60 bytes)
local7.info: Nov 26 15:24:40 BRU-SDW-V5K-01 FTMD[2202]: %Viptela-BRU-SDW-V5K-01-ftmd-6-INFO-
1400002: Notification: 11/26/2019 14:24:40 interface-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 if-name:"ipsec1" new-state:up
local1.info: Nov 26 15:24:40 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/vpn}interface-state-change
local1.info: Nov 26 15:24:44 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}unlock attrs: nc:message-id="12"
local1.info: Nov 26 15:24:44 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 unlock target=candidate
attrs: nc:message-id="12"
local1.info: Nov 26 15:24:44 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="12"
local1.info: Nov 26 15:24:46 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 close-session attrs:
nc:message-id="13"
local1.info: Nov 26 15:24:46 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="13"
auth.info: Nov 26 15:24:47 BRU-SDW-V5K-01 sshd[27428]: Received disconnect from 10.10.10.253
port 40555:11: Closed due to user request.
auth.info: Nov 26 15:24:47 BRU-SDW-V5K-01 sshd[27428]: Disconnected from user vmanage-admin
10.10.10.253 port 40555
authpriv.info: Nov 26 15:24:47 BRU-SDW-V5K-01 sshd[27423]: pam_unix(sshd:session): session
closed for user vmanage-admin
local7.warn: Nov 26 15:24:47 BRU-SDW-V5K-01 BGP.1[6505]: 10.0.0.1 unrecognized capability code:
```

```
70 - ignored
local7.info: Nov 26 15:24:47 BRU-SDW-V5K-01 BGP.1[6505]: %ADJCHANGE: neighbor 10.0.0.1 Up
local7.info: Nov 26 15:24:47 BRU-SDW-V5K-01 CFGMGR[2195]: %Viptela-BRU-SDW-V5K-01-cfgmgr-6-INFO-
1400002: Notification: 11/26/2019 14:24:47 bgp-peer-state-change severity-level:major host-
name:"BRU-SDW-V5K-01" system-ip:10.10.10.242 vpn-id:1 peer:10.0.0.1 bgp-new-state:established
local-address:10.0.0.2 local-routerid:10.10.10.242 peer-routerid:192.168.9.1
local1.info: Nov 26 15:24:47 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/vpn}bgp-peer-state-change
```

Faites particulièrement attention à ces lignes :

```
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 /viptela-vpn:vpn/vpn-instance{0}/interface{ge0/0}/description set to "mpls"
local1.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 commit
thandle 4552 /viptela-vpn:vpn/vpn-instance{1}/interface{ipsec1}/ike/authentication-type/pre-
shared-key/pre-shared-secret set to "*****"
```

Malgré le fait que seule la description de l'interface est modifiée dans le tempate, la clé d'interface ipsec1 a également été mise à jour pour une raison quelconque.

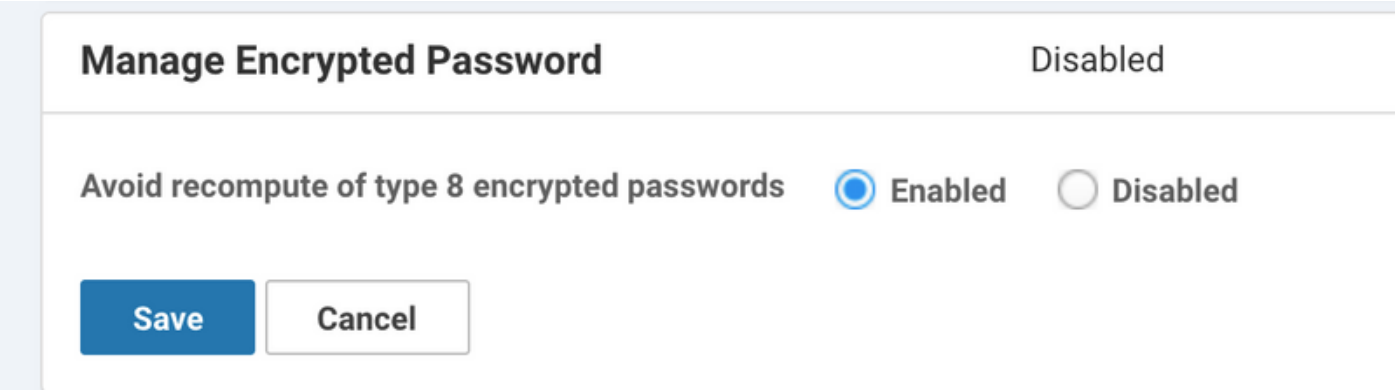
Solution

1. Tout d'abord, il est actuellement impossible d'éviter un tel problème si le modèle de périphérique vManage basé sur les modèles de fonctionnalités est utilisé. Les modèles de fonctionnalités vManage utilisent un mot de passe en texte clair et, en raison de la nature du hachage de type 8, il est régénéré chaque fois qu'une modification est apportée au modèle. Vous devez donc passer aux modèles CLI avec les versions logicielles actuelles. Le hachage de type 8 est un texte chiffré commençant par des symboles 8.

Ce comportement est documenté sous l'identificateur de défaut CSCvn20971

Une demande d'amélioration est également ouverte pour les modèles de fonctionnalités CSCvr86574

2. Si des modèles de périphériques basés sur CLI sont utilisés, le problème peut être évité si le hachage de type 8 est spécifié dans la configuration du périphérique au lieu du mot de passe en texte clair. En outre, le paramètre **Gérer le mot de passe chiffré** dans les paramètres vManage doit être défini sur **Activé** afin d'éviter le recalcul des mots de passe chiffrés de type 8. Vous pouvez le trouver sous **Administration >Paramètres.**



Une fois appliqué, vous pouvez repousser le modèle. Cela provoque le blocage du tunnel pour la dernière fois, car il doit être mis à jour la dernière fois après cela et synchroniser vManage et le périphérique. Presque au moment de toutes les tentatives suivantes, le tunnel reste stable et les modifications sont apportées à la partie pertinente de la configuration uniquement :

```
local1.info: Nov 26 15:42:37 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1267 commit
thandle 4651 begin
local1.info: Nov 26 15:42:37 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1267 commit
thandle 4651 /viptela-vpn:vpn/vpn-instance{0}/interface{ge0/0}/description set to "MPLS"
local1.info: Nov 26 15:42:37 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1267 commit
thandle 4651 end
```

Dans la section suivante, vous trouverez la configuration appropriée pour IPSec basé sur IKE site à site dans le VPN de service à titre de référence.

Configurations

Vous trouverez ici la configuration des périphériques à des fins de référence.

Routeur vEdge :

```
vpn 1
 router
  bgp 65001
   neighbor 10.0.0.1
    no shutdown
    remote-as 65000
   !
  !
 !
 interface ipsec1
  ip address 10.0.0.2/30
  tunnel-source-interface ge0/0
  tunnel-destination      192.168.9.1
  ike
   version      1
   mode         main
   rekey        14400
   cipher-suite aes128-cbc-sha1
   group        2
   authentication-type
    pre-shared-key
     pre-shared-secret $8$cFG/IiaNKkFYXGiHiTCbDEQYcCL4tx1tEhcDh1kO93fzNgc4LDSIIqESFeC6//yU
     local-id          192.168.9.242
     remote-id         192.168.9.1
    !
   !
  !
  ipsec
   rekey                   3600
   replay-window           512
   cipher-suite            aes256-cbc-sha1
   perfect-forward-secrecy group-2
  !
  no shutdown
 !
```

```
!
```

Cisco IOS® :

```
router bgp 65000
 bgp log-neighbor-changes
 neighbor 10.0.0.2 remote-as 65001
!
crypto keyring KR
  pre-shared-key address 0.0.0.0 0.0.0.0 key testtesttesttest
!
crypto ipsec profile IPSEC_PROFILE
 set transform-set TSET
 set pfs group2
 set isakmp-profile IKE_PROFILE
!
crypto isakmp profile IKE_PROFILE
   keyring KR
   self-identity address
   match identity address 0.0.0.0
!
interface Tunnel1
 ip address 10.0.0.1 255.255.255.252
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 192.168.9.242
 tunnel protection ipsec profile IPSEC_PROFILE isakmp-profile IKE_PROFILE
!
```

> **Conseil** : en raison des améliorations apportées à la sécurité dans vEdge depuis la version 19.1 du logiciel, une clé pré-partagée doit comporter au moins 16 caractères.