

El túnel de sitio a sitio IPSec se inestabiliza cada vez que se realiza cualquier cambio en la plantilla de dispositivo

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Configuraciones](#)

Introducción

Este documento describe el problema típico que ocurre cuando los túneles IPSec basados en el intercambio de claves de Internet (IKE) de sitio a sitio (o también conocidos comúnmente como LAN a LAN) se inundan en cada actualización de plantilla de dispositivo en un controlador vManage, explica las causas principales y proporciona una solución para el problema.

Problema

El túnel IPSec basado en IKE parpadea cada vez que la plantilla de dispositivo se actualiza en vManage. Los cambios no pueden estar relacionados con el túnel IPSec de sitio a sitio basado en IKE, pero hacen que el túnel se inunde. El problema puede exponerse aún más si, por ejemplo, el peering eBGP se ejecuta sobre el túnel IPSec. Debido al seguimiento de la interfaz eBGP, el vecino también se inestabiliza y, como consecuencia, se retiran todas las rutas y luego se vuelven a instalar. Esto provoca la interrupción del tráfico a su vez. Por ejemplo, este es el único cambio realizado en la plantilla, tal como lo confirma config-Preview como se muestra en la imagen.

66	66	interface ge0/0
67		description MPLS
	67	description mpls
68	68	ip address 192.168.9.242/24
69	69	ipv6 dhcp-client
70	70	tunnel-interface
71	71	encapsulation ipsec
72	72	color private1 restrict

Así se ve en los registros:

```
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
```

Como puede ver, el vecino BGP ha parpadeado. En `/var/log/messages` puede ver más información:

```
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:ySiw9uiBxffv6HrO0iwDE3jm05mm04IQoc+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)
local11.info: Nov 26 15:24:38 BRU-SDW-V5K-01 confd[1310]: audit user: vmanage-admin/1232 assigned to groups: vmanage-admin,log
local11.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
local11.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"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-id="1"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply, attrs: nc:message-id="1"
local11.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"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-id="2"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply, attrs: nc:message-id="2"
local11.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"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-id="3"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply, attrs: nc:message-id="3"
local11.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"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 get attrs: nc:message-id="4"
local11.info: Nov 26 15:24:39 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply, attrs: nc:message-id="4"
local11.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
'ipsecl_1'
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 07[CFG] vici terminate IKE_SA 'ipsecl_1'
daemon.info: Nov 26 15:24:39 BRU-SDW-V5K-01 charon: 06[IKE] closing CHILD_SA child_ipsecl_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_ipsecl_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_ipsecl_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_ipsecl_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 ipsecl 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]

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
local11.info: Nov 26 15:24:40 BRU-SDW-V5K-01 confd[1310]: netconf id=38 sending notification
{http://viptela.com/vpn}interface-state-change
local11.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"
local11.info: Nov 26 15:24:44 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 unlock target=candidate
attrs: nc:message-id="12"
local11.info: Nov 26 15:24:44 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 sending rpc-reply,
attrs: nc:message-id="12"
local11.info: Nov 26 15:24:46 BRU-SDW-V5K-01 confd[1310]: netconf id=1232 close-session attrs:
nc:message-id="13"
local11.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
```

Preste especial atención a estas líneas:

```
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 "****"
```

A pesar del hecho de que solamente se cambia la descripción de la interfaz en el template, la clave de interfaz ipsec1 también se actualizó por alguna razón.

Solución

1. En primer lugar, actualmente no es posible evitar este problema si se utiliza la plantilla de dispositivo vManage basada en plantillas de funciones. Las plantillas de funciones de vManage utilizan una contraseña de texto sin cifrar y, debido a la naturaleza del hash de tipo 8, se regenera cada vez que se realiza algún cambio en la plantilla, por lo que debe cambiar a plantillas de CLI con las versiones de software actuales. El hash de tipo 8 es un texto cifrado que comienza con símbolos \$8\$.

Este comportamiento se documenta con el identificador de defecto [CSCvn20971](#)

Además, se abre una solicitud de mejora para las plantillas de funciones [CSCvr86574](#)

2. Si se utilizan plantillas de dispositivos basadas en CLI, se puede evitar el problema si se especifica hash de tipo 8 en la configuración del dispositivo en lugar de contraseña de texto sin cifrar. Además de esto, la configuración **Administrar contraseña cifrada** en la configuración de vManage se debe establecer en **Habilitado** para evitar la repetición de las contraseñas cifradas de tipo 8. Esto se puede encontrar en **Administration > Settings**.

Manage Encrypted Password Disabled

Avoid recompute of type 8 encrypted passwords Enabled Disabled

Save **Cancel**

Una vez aplicada, puede volver a pulsar la plantilla. Esto hace que el túnel sea inestable por última vez porque debe actualizarse la última vez después de esto y sincronizar vManage y el dispositivo. Casi en el momento de todos los intentos posteriores, el túnel permanece estable y los cambios se realizan solamente a la parte relevante de la configuración:

```
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
```

En la siguiente sección, puede encontrar la configuración relevante para IPSec de sitio a sitio basado en IKE en VPN de servicio para referencia.

Configuraciones

Aquí puede encontrar la configuración del dispositivo con fines de referencia.

Router 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
!
```

Consejo: Debido a las mejoras de seguridad en vEdge desde la versión de software 19.1, una clave previamente compartida debe tener al menos 16 caracteres.