디바이스 템플릿을 변경할 때마다 IPSec Site-to-Site 터널 플랩

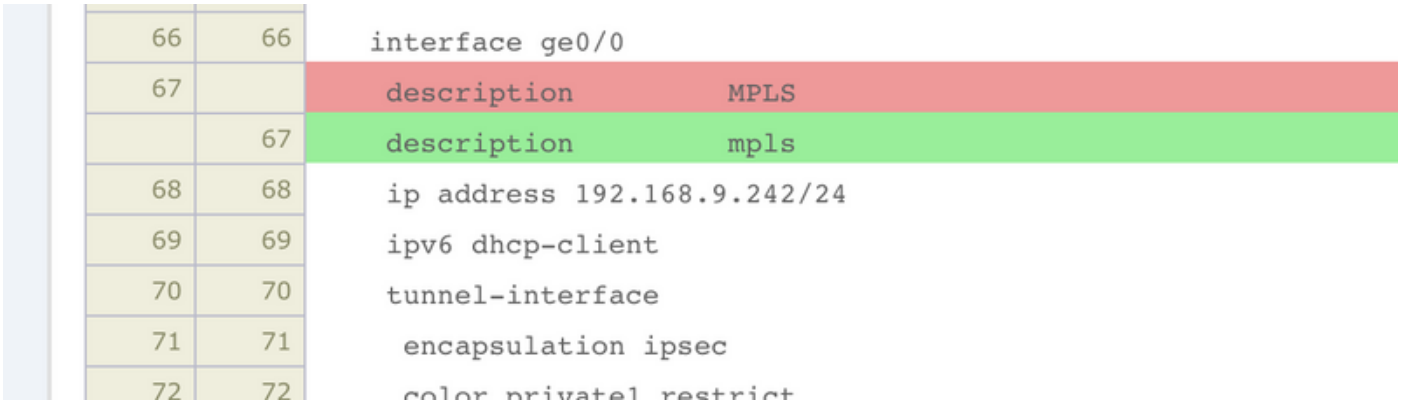
목차

소개

이 문서에서는 vManage 컨트롤러의 모든 디바이스 템플릿 업데이트 시 사이트 간(또는 일반적으로 LAN-to-LAN) IKE(Internet Key Exchange) 기반 IPSec 터널 플랩이 발생할 때 발생하는 일반적인 문제에 대해 설명하고 근본 원인을 설명하고 문제를 해결할 수 있는 솔루션을 제공합니다.

문제

디바이스 템플릿이 vManage에서 업데이트될 때마다 IKE 기반 IPSec 터널이 플랩됩니다.변경 사항은 IKE 기반 사이트 대 사이트 IPSec 터널과 관련될 수 없지만 터널이 플랩됩니다.예를 들어, eBGP 피어링이 IPSec 터널을 통해 실행되는 경우 문제가 더 심각해질 수 있습니다.eBGP 인터페이스 추적 때문에 네이버도 플랩을 수행하여 모든 경로가 철회된 다음 다시 설치됩니다.이로 인해 트래픽이 차례로 중단됩니다.예를 들어, 이미지에 표시된 대로 컨피그레이션 미리보기에서 확인한 템플릿만 변경됩니다.



다음은 로그에서의 모양을 보여줍니다.

```
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
```

보시다시피 BGP 인접 디바이스가 플랩되었습니다./var/log/messages에서 더 많은 정보를 볼 수 있습니다.

```
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
```

해당 행에 대해 구체적으로 주목하십시오.

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

tempate에서 인터페이스 설명만 변경되었지만 어떤 이유로 ipsec1 인터페이스 키도 업데이트되었습니다.

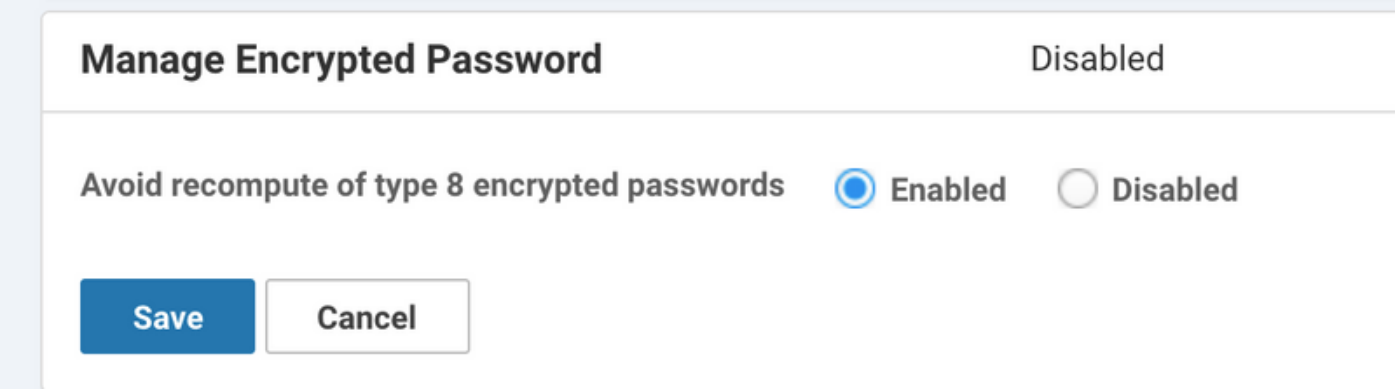
솔루션

1. 먼저 기능 템플릿을 기반으로 하는 vManage 디바이스 템플릿을 사용하는 경우 현재 이러한 문제를 방지할 수 없습니다.vManage 기능 템플릿은 일반 텍스트 암호를 사용하며, 형식 8 해시의 특성으로 인해 템플릿을 변경할 때마다 다시 생성되므로 현재 소프트웨어 버전의 CLI 템플릿으로 전환해야 합니다.Type 8 해시는 8 기호로 시작하는 암호 텍스트입니다.

이 동작은 결함 식별자 CSCvn20971에 설명되어 있습니다.

또한 기능 템플릿 CSCvr86574에 대한 개선 요청이 열립니다

2. CLI 기반 디바이스 템플릿을 사용하는 경우 일반 텍스트 비밀번호 대신 디바이스 컨피그레이션에 지정된 8 유형의 해시가 있으면 이 문제를 방지할 수 있습니다.이 외에도, 유형 8의 암호화된 비밀번호를 재계산하지 않으려면 vManage 설정에서 Manage Encrypted Password 설정을 Enabled로 설정해야 합니다.이는 Administration(관리) **>Settings(설정)** 아래에서 찾을 수 **있습니다.**



적용된 후에는 템플릿을 다시 한 번 푸시할 수 있습니다.이렇게 하면 터널이 마지막으로 플랩될 수 있습니다. 이 후 마지막으로 업데이트하고 vManage 및 디바이스를 동기화해야 하기 때문입니다.모든 후속 시도가 있을 때 터널은 안정적인 상태로 유지되며 컨피그레이션의 관련 부분만 변경됩니다.

```
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
```

다음 섹션에서는 서비스 VPN에서 사이트 간 IKE 기반 IPSec의 관련 컨피그레이션을 참조할 수 있습니다.

구성

여기에서 참조용으로 디바이스 컨피그레이션을 찾을 수 있습니다.

vEdge 라우터:

```
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
!
```

팁: 19.1 소프트웨어 버전 이후 vEdge의 보안 개선 사항으로 인해 사전 공유 키는 16자 이상이어야 합니다.