

天翼云・SSL VPN

安全加固操作指南

天翼云科技有限公司

2022年7月



2	第1章 前言
2	第2章 准备工作
2	2.1 事前准备
口开启关闭方法 2	2.2 设备升级开放站
4	2.3 设备加固
4	2.3.1 补丁包实施
	第3章 注意事项



第1章 前言

已知问题,近日天翼云在持续的产品加固自查过程中发现的,天翼云 SSL VPN 设备存在 一个安全风险可被攻击者利用。对此,天翼云已推出安全补丁,强烈建议您在服务人员的协 助下立即进行排查验证和补丁修复提前整理升级方案。

第2章 准备工作

2.1 事前准备

- 1、Windows PC 一台,用于升级,巡检等操作
- 2、补丁包 Security-reinforcement-patch-package.rar
- 3、升级工具 SANGFOR_Updater6.1

补丁包及工具下载地址:

https://oos-cn.ctyunapi.cn/downfile/2022download/SANGFOR_Updater6.1.zip

https://oos-cn.ctyunapi.cn/downfile/2022download/Security-reinforcementpatch-package.rar

2.2 设备升级开放端口开启关闭方法

51111 端口

对应服务:升级服务

关闭影响:不能通过升级服务客户端进行远程升级,仅关闭了外网的使用,不影响内网

注意事项:安全组需要放 51111 端口权限

开启方法:通过升级客户端升级加固补丁,需开启 51111 升级客户端:

方法一:登录 SSLVPN 控制台【系统设置】-【系统配置】-【运维配置】- 升级维护 勾选"启用 LAN 口临时访问",然后点击保存。



	6.8 RI 您还可以免费试用80天;您可以使用 在线授权 或 本地授权服务器授权 空间 社区疑问、资料搜索
<mark>控制台 ↓ 这行状态 ◆ 熟錄设置</mark> → 系統配置 → 网络图: 【	授权信息 日期与时间 控制台配置 外围数据中心 设备证书 邮件服务器 Sysles 安全感知设置 SMUE 送维配置 ご 近程维护 ③ ● 倉用24小时 ● 长期启用 ● 募用 ご 計級维約
 > 时间计划 > 位置管理 > 管理员帐号 4 SSL VFN选项 > 系统选项 	□ 倉用LAN口協封访问 □ 含用TAN口協封访问 □ 含用TAN口協封访问 □ 自用TAN口協封访问 □ 自用TAN口協封访问
 > 网络传输优化 > 主肠管理 > 集群部署 > 分布式部署 	保存 取消

方法二:则需使用 IE 浏览器在①【系统设置】-【系统配置】-【控制台配置】- 启用远

程维护支持;②在【防火墙设置】-【过滤规则设置】-【本机规则】- 启用允许外网使用 升级客户端进行维护。

	. 6. 3 R2		在线咨询 社区疑问、资料搜	🛣 Q 🧘 🧘 admin 🔻	▶ 个人设置 查看帮助
控制台	≫ 防火墙本机规则				(2) 翌勤
▶ 运行状态	描述			操作	
 系统设置 	允许外网到本机的ping和tri	icert		 自用 	○ 禁用
▶ SSL VPN设置	允许外网邀录本机的Mad				 禁用
→ C设置	允许外网使用升级客户端进行	5维护		● 启用	○ 禁用
▶ PSec VPN设置					
▼ 防火墙设置		确定		白田氏占土确实	
> 网络 器)	口用归品证明化	
→ IP组→置					
⊿ 过速、则设置					
> 本机规则	•				
> LAN<=>DMZ					
> DMZ<=>WAN					
> WAN<->LAN					
> VPN<->LAN					
> VPN<->WAN					

有该界面出现,表示端口打开成功

SANGFOR SSL MT. 6. 8 R2	▲发帖求助 ■	在线咨询 化区第	间、资料搜索 Q	🚊 admin 🔻	个人设置 查看帮
控制台					
▶ 运行状态					
> 系统设置					
→ SSL VPN设置					
→ sc设置					
 IPSec VPN设置 					
▼ 防火墙设置					
> 网络服务设置	 SANGFOR				
→ IP组设置					
▲ 过速规则设置					
> 本机规则	保存配置成功				
> LAN<->DMZ	10.00				
> DMZ<->WAN	返回				
> WAN<->LAN					
> VPN<->LAN					
> VPN<->WAN					



2.3 设备加固

2.3.1 补丁包实施

2.3.1.1 安全加固包

支持版本范围: 7.5

M5.0-M768R2

补丁包影响范围

SP_SSL_AW_01 :

M7.5及以上版本:升级会重启svpn服务,用户会重连导致无法访问资源,影响时间3分钟 左右;

SP_SSL_WD_04 :

升级会重启 boa 服务,影响 VPN 控制台登录和访问,影响时间:1分钟;但不影响客户业务

补丁包实施流程

1、准备升级环境

1)准备一台安装 Windows 操作系统的 PC,连接 VPN 设备 LAN 口或者公网 IP;

2、实施流程

如果是单台设备,直接升级即可

如果是集群环境,无需拆集群,直接在分发器上升级,真实服务器会自动同步升级,

如果是分布式环境,先升级主节点,再升级从节点;如果节点是本地集群部署,按 集群环境升级即可

1) 设备实施流程

首先使用升级客户端 Sangfor Updater 6.1 加载相应的补丁包的 Check 包检测补丁包 的是否与其他补丁或定制冲突, Check 包加载完成显示升级成功后,再加载补丁包;补丁包 加载完成提示升级成功后,查看设备版本信息有对应的补丁包字段即完成实施。

(1) 打开升级客户端, 输入 SSL 设备 IP 地址和控制台超级管理员 admin/Admin 的密

4



码,然后连接设备。

🗟 SANGFOR设备	升级系统 - 设备未连接	
	IGFOR	
输入超	级管理员Admin/admin的密码	
设备IP地址:	10. 2. 3. 240 🗸	查找设备 (S)
管理员密码:	****	
	🗹 记住密码	
选项(0)		连接©

(2)选择从本地加载补丁包的 Check 补丁包,点击 下一步 按钮。

SANGFOR设备升级系统 - 10						×
SANGFOR	查找范围([):	加固包		- G 👂 📂 🗔	•	
	名称	^	1	修改日期 2019/3/25 15:06 2022/7/28 22:29	类型 文件夹 CSII 文件	
===□反面目云: 版本: M7.6.8 R1 IP: 10.	SP_SSL_WD	(_01_signed.ssu 0_04_CHECK_signed.ssu 0_04_signed.ssu	2 3 4	2022/7/28 22:29 2022/7/28 22:29 2022/7/28 22:29 2022/7/28 22:29	SSU 文件 SSU 文件 SSU 文件 SSU 文件	
Q备升级 ○ 本世刊作	《		(>
选择版本(S)	文件名(N): 文件类型(I):	Sangfor UpdatePacka	age Files (*.ssu	;*.cssu)	打开(<u>O</u>) / 取消	
◉ 从本地加载升级包		□以只读方式打开(<u>R</u>)				
断开连接(D)	浏览(B) 步(N)				

(3)再次确认升级,点击 确认升级。



SANGFO	R设备升级系统	设备未连接	_		×
	SANG	FOR	按F10打开技;	术支持工具	
当前沿各位	确定升级?			×	
当前反面に 版本: ID·	当前版本: M7.6.8 F 升级版本: SANGFOR-	1 —SP_SSL_AW_Check			
U. 设备升级-	版本说明: 此升级包 不需要格 升级提示] 升级完不需要重启 :测软件升级授权 :信息 !	í	^	
	功能: 1、安全; 	加固		~	
◎ 从本 G:\	work(sangtor	בר ז - 1 -2022) נא ב וציאייתני	取消(C)	刘贲(B)	
断开连接(D)			下一步(1	N)

(4)确认升级后,等待一段时间,会提示升级完成,则代表检测通过,可以实施补丁包。

SANGFOR设备升级系统 - 设备未连接		☑ 技术支持工具 - 设备未连接
		升级(U) 备份(B) 时间(T) 命令(C) 帮助(H)
	按F10打开技术支持工具	保存在 D:\工具\SANGFOR_Updater6.1\SANGFOR_Updater6.1\ST ~ 备份配置完成!
当前设备信息 版本: M7.6.8 K2 IP: 192.200.244.116		止住准爾可知 D:\1_L\5ANGFOR_Updater6.1\SANGFOR_Updater6.1\STARTUP\ 准备升级完成 正在上载升级文件
设备升级 【状态: 升级成功		D:\工具\SANGFOR_Updater6.1\SANGFOR_Updater6.1\SIARIUP\ D:\工具\SANGFOR_Updater6.1\SANGFOR_Updater6.1\SIARIUP\ 上载升级文件1完成 开始升级,请等候
详细信息:		完成! 升级完成。 与设备连接中断,请重新连接
	断开连接 (2)	▼ ▼ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

(5)点击断开连接,再次重新连接上设备后,选择补丁包,点击下一步加载升级



	A +71			~
SANGFOR	11/16			^
按F10打开排	査 査 找 范 围(∐):		· G 🗗 🖻 🔛	•
	名称	^	修改日期	类型
当前设备信息	STARTUP		2019/3/25 15:06	文件夹
版本。 M7.6.9.P1	SP_SSL_AV	<u>V_01_CHECK_signed.ssu</u>	2022/7/28 22:29	SSU 文件
	SP_SSL_AV	N_01_signed.ssu	2022/7/28 22:29	SSU 文件
IP:	SP SSL W	D_04_CHECK_signed.ssu	2022/7/28 22:29	SSU 文件 SSU 文件
设备升级	0.000	D_04_signedissu		555 XIF
	<			>
	文件名(N);	SP SSL AW 01 signed.ssu		打开(0)
选择版本(S)				111/(0)
● 从本地加载升级句	文件类型(工):	Sangfor UpdatePackage Fi	les (*.ssu;*.cssu)	~ 取消
		□以只读方式打开(R)		
川面包\SP_SSL_AW_0				
断开连接(D)	下一步(N)			
(6)再次确认升级,点击 开始升级	ξ. o			
┃ 🐨 SANGFOR设备升级系统 - 设备未连接				\square \times
SANGFOR				+
			按F10打开技术支持	守上具
确宁升级2			~	
WOAE/TAX:			^	
当前设备倡				
ゴ閉線牛・				
版本: M7.6.8 Kl				
升级版本:				
ID. SANGFOR-SP_SSL_AW				
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●				
山口、山谷、山山、山山、山山、山山、山山、山山、山山、山山、山山、山、山、山、山	重启		<u>^</u>	
不需要检测软件升级授	权			
→ → → → → → 升级提示信息!				
2, 定合加固				
1、女主加回				
			×	
◎ 从本		TT #441472 (11)	期 2当(c)	
			取用(四)	
			-	
G: WOLKSSHOLD SERVE PARTY	24070			\$(R)
G:\work(sangtor),	241/320	고 (까지 프 (아드) 아	L_AW_O XUG	ጀ(B)
G:\work\sangtor\37-9913#37202	2 417 20			ቼ(B)
G:\ <mark>พอเหาุรลกฎาธา เว~พฐา 1 20</mark> 1/202	.2417320	가드 (VII의 단 / 3F_33		ቼ(B)
G:\\work\sangtor\ว~พราว พว\zoz	.2417320	고 (까따먹 문 / 3 3-3		ັະ(B)
G:\\work\sangtor\ภ~พฐาวพูว\202	.2477320	고 까띠먹 말 (하는 33		ຣັ(B)
G:\\work\sangtor\;>>>>y)zoz	.2417320	고 까뜨린 (가드 33		5(B)
G:\\\work\\sangtor\\;>>>>y\zvz 断开连接(D)	.2477720	고 까뜨린 (가드 33		琶(B) 下一步(N)

(7)确认升级后,等待一段时间,提示升级完成,补丁包完成升级。



s/	ANGFOR	按F10打开技术支持工
当前设备信息	2	
版本:	M7.6.8 R2	
IP:	192.200.244.116	
设备升级		
状态:	升级成功	
详细信息:	71 级元风 °	*
	设备已经断开	*
	<	Þ

(8)点击断开连接,再次重新连接上设备后,选择补丁包,点击下一步加载升级,通过升级工具加载 SP_SSL_WD_04_CHECK_signed.ssu 包升级,检查当前设备是否能升级(返回"升级完成"即说明可以升级此次补丁包,否则当前设备不支持升级此次补丁包)

🚱 SANGFOR设备升级系统 - 设备未连接 —					
	💿 打开				×
SANGFOR 按F10打开挟	查找范围([):	山固包	- G 👂 📂 🛄	-	
当前设备信息 版本: M7.6.8 R1 IP: 10 设备升级 ① 在线升级 	名称 SP SSLAW SP SSLAW SP SSLAW SP SSLWD SP SSLWD SP SSLWD 文件名(N): 文件类型(D:	01_CHECK_signed.ssu 01_signed.ssu _04_CHECK_signed.ssu _04_signed.ssu SP_SSL_WD_04_CHECK_signed.ss Sangfor UpdatePackage Files (*.	修改日期 2019/3/25 15:06 2022/7/28 22:29 2022/7/28 22:29 2022/7/28 22:29 2022/7/28 22:29 u ssu;*.cssu) 、	 类型 文件夫 SSU 文件 SSU 文件 SSU 文件 SSU 文件 SSU 文件 第 打开(2) 取消 	*
斯开连接(D)	下一步(N)				

(9)点击断开连接,再次重新连接上设备后,选择补丁包,点击下一步加载升级,通过升级工具加载 SP_SSL_WD_04_signed.ssu 包升级,检查当前设备是否能升级(返回"升级完成"即说明可以升级此次补丁包,否则当前设备不支持升级此次补丁包)



G SANGFOR设备升级系统 - 设备未连接 −				
SANGFOR	⑥ 打开			
	查找范围(<u>l</u>):	📙 加固包	~ 🕝 🌶 📂 🖽	•
	名称	^	修改日期	类型
当前设备信息	STARTUP		2019/3/25 15:06	文件夹
	SP_SSL_AV	V_01_CHECK_signed.ssu	2022/7/28 22:29	SSU 文件
版本: M17.6.8 K1	SP_SSL_AV	V_01_signed.ssu	2022/7/28 22:29	SSU 文件
IP: 1	SP SSL W	0 04 CHECK signed.ssu	2022/7/28 22:29	SSU 文件
	SP_SSL_W	D_04_signed.ssu	2022/7/28 22:29	SSU 文件
设备升级				
○在纬升级	<			>
选择版本(S)	文件名(N):	SP_SSL_WD_04_signed.ssu	1	打开(<u>O</u>)
	文件类型(工):	Sangfor UpdatePackage Files (*.ssu;*.cssu)		
◉ 从本地加载升级包				
		U只读方式打开(R)		
川间型(SP_SSL_AW_0				.11
断开连接(D)	下一步(N)			

2.3.1.2 安全加固完成标志

查看设备的版本信息有对应的补丁包名称 SP_SSL_WD_04、SP_SSL_AW_01,说明升级成

功。



2.3.1.3 补丁包回退

实施完补丁包需验证业务是否有异常,若出现不可控的异常问题,在短时间不能解决的, 应尽快恢复业务,回退方式如下:

appversion 中从下往上依次回滚



集群环境下回滚:不用拆分集群,先回滚分发器,再回滚真实服务器 双机环境下回滚:需要拆分双机,每台设备都需要回滚 分布式环境下回滚:不用拆分分布式,先回滚主节点,再回滚从节点

SP_SSL_WD 包回滚步骤:

回退步骤:

- 1、进入设备后台
- 2、执行命令: cd /hislog/cti-support/SP_SSL_WD/
- 3、执行命令: setsid ./cti-support.sh -roll
- 4、等待15s,回滚操作完成

SP_SSL_AW 包回滚步骤:

回退步骤:

- 1、进入设备后台
- 2、执行命令: cd /hislog/cti-support/SP_SSL_AW/
- 3、执行命令: setsid ./cti-support.sh -roll
- 4、等待15s,回滚操作完成

第3章 注意事项

1、升级完成后需要登录 sslvpn 控制台,关闭升级维护访问选项。

2、安全组放开 51111 端口访问权限需要删除。