华为 eNSP USG6000V 实现 SSL VPN

摘要:

IPSEC VPN可以实现不同局域网之间通过Internet进行VPN连接,一般由网关设备进行VPN连接。 SSL VPN 可以实现员工到公司内部,由员工电脑进行 VPN 连接。一般由员工 Web 登录虚拟机网关手 动连接,或由 SecoClient 客户端自动连接。

本案例以华为 eNSP USG6000V 设备实现 SSL VPN,网络拓扑如下:



一、基本配置

1. 防火基本配置脚本参考

admin Admin@123 y Admin@123 admin@123 admin@123 u t m sys sysn FW1

web-m time 60 user con 0 idl 60 ret sys int g0/0/0 ip add 192.168.20.10 24 serv ena serv https per serv ping per ret

2. 路由器基本配置

#

```
interface GigabitEthernet0/0/0
ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
ip address 192.168.100.254 255.255.255.0
#
```

3. 登录防火墙

https://192.168.20.10:8443

4. 配置防火墙接口

	l uawei SG6000V1-ENSP	∎ 面	板监		「「」の	a l	「 M络	■ 系统		
	-	接口列表	ž							
·● 接口 *C链路		🕂 新建	💢 刪除						69	刷新
	接口组	接口	名称	5	安全区域		1	P地址		
 -• छ中×: ●● 安全区 	地	GE0/	0/0(GE0/METH) t	rust(🕮 defaul	lt)	1	92.168.20.10		
🖳 VXLA	N	GE1/	0/0	t	rust(🕮 public	:)	1	92.168.10.254 		
DNS	肥冬岛	GE1/	0/1	ι	intrust(🗮 pub	olic)	1	00.1.1.1		
Lange Briter	加度力者者	GE1/	0/2	-	- NONE(🕮	public)				
IPSec		GE1/	0/3	-	- NONE(🕮	public)				

5. 配置路由

Huawei HUAWEI USG6000V1-ENS	SP 間面板	「」	L 策略	■す 対象	小 网络	■ 系统	
■ 接口	配置默认优先级						
 □ 接口 ◎ \$\$ 链路接口 ● \$\$ 链路接口组 □ 接口对 ● 安全区域 ■ VXLAN 	IPv4默认, IPv6默认,	优先级 优先级	60 60		<1-255> <1-255>		应用
	静态路由列表						
■ DHCP服分器 ■ 路由	🕂 新建 💥 删除						
■智能选路		目的地	地/掩码 目	的虚拟路由器	下一跳	优先级	出接口
── ❷ 虚拟路由器	public	0.0.0.0	0/0.0.0.0 pu	blic	100.1.1.2	60	
▲静态路由 ④ 都态路由							

6. 配置 NAT

WEI USG6000V1-ENSP	面板	「「「」」	策略	■ 対象	网络	系统	
→ 安全策略	NAT策略	颖转换地址池	目的转换地	址池			
NAT策略	源转换地址池	列表					
	🕂 新建 💢 删除						
₩220版分替映射 ② 服务哭合裁物銜	□ 地址池名称		IP地址范围		端口地址	转换	NAT类型
▶ 带宽管理	NAT池		100.1.1.10-1	00.1.1.16	Ø		五元组NAT
🖁 配额控制策略							
🗅 代理策略							+



7. 配置安全策略

	Huawei USG6000V1-ENSP] 面相	(x		■ 对	⊋ ∎ §2	小 网络	ا چ	】 统					当前用	户: admii
安全	策略 <u> </u>	安全策略	列表												
	王 東 昭 新 昭	🕂 新建安全	全策略 🔶 新	所建安全策略组 💢 🖁	眦除 🗗 复	制 💲 移	;zh• 🕞 j	插入 🛃 🕏	学出 🛛 🔍	清除全部	命中次数	칠 启用	1245日	👿 列定制	禧 展开
😰 服务	器负载均衡														
- 🐶 市兑 - 🕓 配额	官理 控制策略	🔍 请输	入要查询的P	内容	●添加	喧询项									
12 代理	策略	序号	名称	描述	标签	VLA	源安	目的	源地	目的	用户	服务	应用	时间段	动作
🔘 安全	防护	1	CL-1	内网访问外网		any	trust	🕙 untru	sany	any	any	any	any	any	允许
🖺 ASP	F配置	2	default	This is the defa		any	any	any	any	any	any	any	any	any	禁止

8. 验证结果 (此时内网电脑可以访问外部路由)

基础配置 客户端信	息日志信息		
Mac地址:	54-89-98-BA-04-78		(格式:00-01-02-03-04-05)
IPV4配置			
本机地址:	192 . 168 . 10 . 2	子网掩码:	255 . 255 . 255 . 0
网关:	192 . 168 . 10 . 254	域名服务器:	0 . 0 . 0 . 0
PING测试			
目的IPV4:	100 . 1 . 1 . 2	次数:	5 发送
本机状态:	设备启动		ping 成功:5 失败:0
			保存

二、配置 VPN

1. 创建用户

HUAWEI	Huawei USG6000V1-ENSP	日日	公路	ら 策略	「「」	晶网络	系统		
- -	书 [▲] 《 「 本地证书 +	用户管理							
	CA证书	场景 11 用户配置		□ 上网行为	管理 ✔ SSL	VPN接入 🗌 L21	[P/L2TP over IP	Sec IPSec接	:入?
- E	E书过滤	用户所在位置		✓本地		□认证服务器			
□ 및 地: □ @ 地	址 区	本地H户 用户/用户组/表	7全组管理	[守八田戸] 列売		[守八女王祖]			
3 ಿ 腸 3 🔥 应	务 用	♣新建▼ 💥 빠	除國批里	修改 🗗 复制	🔒 导出 🔹 🎎	基于组织结构管理	開户		最大化显
■ & 用.	户 lefault	名称		描述	所属组		来源	绑定信息	
	人证域	└	(別) 页共 1	VPN用户 页 >) 每	A /default 页显示条数 50	~	本地	无	
- 1967 - 1967	A证策略 人证选项	2 _{高级}							
- S JF	月户导入 王线用户	💌 新用户认证	E选项 (新用	户指本地不存在	E的账户)				
3 🖺 终 3 尾 认	端设备 证服务器							应用	
	hitah								

2. 创建认证策略

HU	JAWEI	Huawei USG6000V1-ENSP	■■ 面板		「「」」	上 网络	■ 系统			
	■ こ こ 二 二 二 二 二 二 二 二 二 二 二 二 二	} ▲ ≪ [认证策略列表							
	- ∰C/	地址书 A证书	🕂 新建 💢 删除 📑	复制 🔞 插入 💲 移动•	🌉 清除全部台	命中次数 🖺 启	用 🛃 禁用			
	E CF	RL	🔍 请输入要查询的	内容	◎添加查询项					
	≣ }ùE	书过滤	名称	描述	源安全区域	目的安全	源地址/地区	目的地址/地区	认证动作	Portal
	 地址 地区 	<u> </u>	CL-SSLVPN	SSLVPN登录	Suntrust	etrust	any	any	Portal认证	
	😂 服务	ł	default	This is the default rule	e any	any	any	any	不认证	
Ð,	À 应用	1								
	â 用户	1								
	- 🕵 de	fault								
	િ ઢોત	证域						+	•	
	• िः। •िक्रां।	证策略 证选项								

3. 创建 VPN 虚拟网关

[FW1]v-gateway sslvpn1 interface GigabitEthernet 1/0/1 port 4430 private www.a.com

HUAWEI US	iawei G6000V1-ENSP	■■	「二」	^{策略}	■子 ■ 対象	小 网络	L 系统	
3 📠 接口	~<	SSL VPN 列表						
	¢.	🕂 新建 🐹 删除						
VXLAN		网关名称	网络	关地址:端口		域名		本地证书
🗄 💷 DNS		sslvpn1	10	0.1.1.1:4430		www.a.com		default
🗄 💼 DHCP服	务器							
🛯 🔚 路由								
🗉 🔒 IPSec								
🗄 🤬 L2TP								
😪 L2TP ov	ver IPSec		+					
🗉 🖨 GRE								
SSL VPI	N PN							

4. 修改 VPN 虚拟网关, 网关配置, 端口号此处为方便改为 443, 为安全建议使用其他端口

修改 SSL VPN			
SSL VPN配置	网关名称	sslvpn1	*
🗟 网关配置	类型	 独占型 共享型 	
New SSL 配置	网关地址	GE1/0/1 * 100.1.1.1	* 端口 443 <1024-50000>或443
🗖 📑 资源		提示: 为保证用户登录网关,需要开启3	安全策略。[新建安全策略]
… 🔞 网络扩展	域名🕐	www.a.com	
· 🕼 web代理	用户认证		\sim
	本地证书	defa <u>u</u> it 🗸	
	客户端CA证书	default 🗸	[多选]
🔲 🐻 终端安全	证书认证方式 🕐	NONE 🗸	
	认证域	请选择认证域	
公 缓存清理	DNS服务器	L	
홃 角色授权/用户	首选DNS服务器 🕐		
💩 MAC认证	备选DNS服务器 1		0
🕞 证书过滤		提示: 修改快速通道端口号会导致在线所	」 用户下线
🔲 📃 页面定制	ゆ 速通 道 渡 口 是 🔊	442	-1.400005
"原LOGO定制		445	1-499992
	取入用尸釰	10	<1-200>
	最大并发用户数 	10	<1-100>

新建安全策略								
提示: 新建时可以基于策略模板来快速定义您需要的	的策略。[选择策略模板]							
名称	CL-SSLVPN网关	*						
描述	SSLVPN策略(sslvpn1)引入							
策略组	NONE							
标签 +	请选择或输入标签							
VLAN ID	请输入VLAN ID	<1-4094>						
源安全区域	请选择源安全区域	[多选]						
目的安全区域	local	[多选]						
源地址/地区③	请选择或输入地址							
目的地址/地区??	请选择或输入地址							
用户③	请选择或输入用户	[多选]						
接入方式③	请选择接入方式							
终端设备 🕐	请选择或输入终端设备							
服务 🕐	https ×							
应用	请选择或输入应用	[多选]						

5. 修改 VPN 虚拟网关,网络扩展

修改 SSL VPN		
SSL VPN配置	网络扩展功能通过在客户端安 内网资源就像访问本地局域网	装虚拟网卡,从SSL VPN网关获取虚拟IP地址,实现了对所有基于IF ——样方便。
☆ 网关配置 ■、SSL配置	配置网络扩展	אווויין א
■ 尝 资源 ◎ 网络扩展 + ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	 网络扩展 保持连接 隧道保活间隔 (?) 	 ✓ 启用 120 <10-3600>秒
 ② 文件共享 → 端口转发 ■ 修 终端安全 ▲ 主机检查 ▲ 缓存清理 	可分配IP地址池范围 路由模式	192.168.10.100-192.168.10.150/255.255.255.0 行之间用 10.10.1. 10.10.1. 手动路由模式 ● 修改路由模式和内网网段会导致用户下线
 ▲ 角色授权/用户 ▲ MAC认证 ● 证书过速 ■ ● 页面定制 ● ① LOGO定制 ■ → ○○○○○○○○ 	可访问内网网段列表 该功能是为了灵活控制用户前和本地局域网,不能访问Inte ◆新建 ※ 删除	可访问内网网段的范围,且不影响用户访问本地局域网和Internet。如 ernet。
	 IP网段 192.168.10.0 	子阿淮尚 255.255.255.0

6. 修改 VPN 虚拟网关,网络扩展,新建访问内网安全策略

路由模式	修改网段		×			
	IP网段	192.168.10.0	×			
可访问的	子网掩码	255.255.255.0	*			
该功能是;	提示: 为保证用户使用网	骆扩展,需要开启安全策略。 [新建安全策	略]	t。如果:	不配置,	用户仅能
和本地局I		▲ 确定 B	以消 🔪			
╬ 新建		•		J		
	n R	子阿掩码		\geq	编辑	
✓ 192.1	68.10.0	255.255.255.0			2	
	第 1 页共 1页 〉	> □ 每页显示条数 50 🗸				显示

修改安全策略		
提示: 新建时可以基于策略模板来快速定义您需要的	的策略。[选择策略模板]	
名称	CL-SSLVPN访问内网 *	
描述	VPN电脑访问内网	
策略组	NONE	
标签	请选择或输入标签	
VLAN ID	请输入VLAN ID <1-4094	4>
源安全区域	untrust 👽 修选]	
目的安全区域	trust 👽 修选]	
源地址/地区 🕐	any ×	
目的地址地区③	192.168.10.0/255.255.255.0 ×	
用户②	any x [多选]	
接入方式③	any ×	

7. 查看安全策略

Huawei Huawei USG6000V1-ENSF	。 面板	「二」	■ 策略 対象		回 系统				当前用户	₹: admin	提交保	存報	り 关于 🛚	多改密码 注
 □ 診 安全策略 ○ 安全策略 □ □ PAT策略 □ □ NAT策略 □ 診 服务器负载均衡 	安全策略	刘表 策略 ♣ 新建安全策略约	3 💥 刪除 💣 复制] 💠 移动 🖷 插)) 🔒 导出	▼ ■ 清除全	言部命中次数 📑	启用 🚹	禁用 🐻 列定制 🗄	■展开 詣	回 し し し し し し の の の の の の の の の の の の の	新 💽 命	中查询 💼	■清除命中:
 ······ ···· ···	🔍 请输)	要查询的内容	◎添加	查询项										
12 代理策略	序号	名称	描述	标签	VLA	源安全	目的安全区域	源地	目的地址/地区	用户	服务	应用	时间段	动作
 □ □	1	CL-1	内网访问外网		any	Utrust	Suntrust	any	any	any	any	any	any	允许
ter ASPF配置	2	CL-SSLVPN网关	SSLVPN策略(ss	ivpn1)引入	any	any	Slocal	any	any	any	https	any	any	允许
	3	CL-SSLVPN访问内网	VPN电脑访问内	网	any	Suntrust	trust	any	192.168.10.0/	any	any	any	any	允许
	4	default	This is the defau	ilt rule	any	any	any	any	any	any	any	any	any	禁止

三、员工从外网使用 SecoClient 客户端登录,一般用于经常性访问

1. 下载 SecoClient 客户端,并按默认安装

参考链接: https://wwi.lanzoup.com/ifKHc0mhwzsf

2. 配置 VPN 相关参数



3. 连接到公司网络

🔋 登录			×
Se	coClient		HUAWEI
服务器地址 一登录信息	100.1.1.1:443		▼ □ 自动
用户名:	vpnu1		
密码:	•••••		
	☑ 记住密码	☑ 自动登录	
	登录		

4. 启动成功后,员工电脑正常访问公司内网,电脑桌面右下角出现 SecoClient 客户端图标及相关信息

1	SecoCl 连接成J Huawei \	ient 力 /PN(Clien	t					
	Å	^	1	۳.	⊲ »)	英	16:10	垦	

- 四、员工从外网使用 Web 方式认证,并进行 SSL VPN 登录,一般用于临时性访问
- 1. 使用 IE 浏览器访问 VPN 网关, https://100.1.1.1, 按提示安装控件
 - 注:因浏览器兼容性原因,需要使用 Windows 10 的 IE 浏览器



2. 登录进行 SSL VPN 认证, 输入 vpnu1 用户名和密码

			★ 收藏
	🌲 vpnu1		
SSL VPN	a		
HUAWEI	◎中文	~	
下载并安装证书可以为您消除安全警告提示框,并有助于加快您的访问速度。 <u>如何安装证书?」点此下载证书</u> 如果您使用的是USB Key证书认证,请先插入USB Key 再访问本页面或插入USB Key后刷新本页面。	登录		

3. 启动"网络扩展",期间弹出 SVN 网络客户端 (SVN Network Extension Client)安装界面,单击

"是"进行安装



(=) (2) https://100.1	1.1.1/main.html?&	▼ 😵 证书错误 🖒	搜索	ー ロ × の☆隠 ⁹
🥖 welcome	×			
Sk ssi v				俞 主页 🚨 用户 🔨
	ドN 当前用户: vpnu:			登录时间:1098661接地址:
welcom	e			
▼ 网络	扩展			
启动				
点击按钮启	品动业务后可以访问内网资源。			
		+		

4. 启动成功后,员工电脑可以正常访问公司内网,电脑桌面右下角出现 SVN 客户端图标及相关信息

	▶ 命令提示符
M (icrosoft Windows [版本 10.0.17763.316] c) 2018 Microsoft Corporation。保留所有权利。
С	:\Users\amm>ping 192.168.10.2
고갑자자자	E在 Ping 192.168.10.2 具有 32 字节的数据: 青求超时。 长自 192.168.10.2 的回复: 字节=32 时间=49ms TTL=254 长自 192.168.10.2 的回复: 字节=32 时间=38ms TTL=254 长自 192.168.10.2 的回复: 字节=32 时间=22ms TTL=254
1 往	92.168.10.2 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失), 主返行程的估计时间(以毫秒为单位): 最短 = 22ms, 最长 = 49ms, 平均 = 36ms

