

PULSE SECURE SSL VPN

配置手册

jinchutou.com



Microshield Technology Co., Ltd

北京市海淀区西三环北路 50 号豪柏大厦 C2 座 18-19 层 100048

电话: (86)10-88518768

www.microshield.com.cn

目录

一、 初始化设置	3
1.1、通过 Console 连接 ssl vpn.....	3
1.2、使用浏览器连接 SSL VPN.....	5
二、 SSL VPN 基本设置	6
2.1、网络接口更改.....	6
2.2、添加用户认证服务器.....	7
2.3、添加 SSL VPN 的认证域	8
三、添加角色及角色映射	9
3.1、添加角色.....	9
3.1.1 用户角色 CDH-Finance	9
3.1.2 用户角色 CDH-Cephei.....	11
3.1.3 用户角色 CDH-WM.....	12
3.1.4 用户角色 CDH-CDH.....	13
3.2 角色映射	14
3.3 基于 realm 的 URL.....	15
四、资源访问控制	16
4.1 新建 NC 隧道地址池	16
4.1.1 添加内置数据库认证	16
4.1.2 配置 Admin Realm	17
4.1.3 用户角色	18
4.1.4 角色映射	22
4.1.5 角色映射及 profiles 定义规则.....	25
4.2 新建 NC 隧道地址池	26
4.2.1 添加 LDAP 认证方式.....	27
4.2.2 用户 Realm 配置	28
4.2.3 用户角色 Temp-Temp.....	29
4.2.4 角色映射新建 Rule	30
4.3 新建 NC 隧道地址池.....	32
4.4 定义 realm 登陆方式	33
五、书签配置	34
六、Signing In 登录配置	34

一、 初始化设置

1.1、通过 Console 连接 sslvpn

SSL VPN 的初始化是通过设备的 Console 端口完成的，Console 的设置如下：
9600, 8, N, 1。

在管理员的计算机上使用任意终端软件，包括 HyperTerminal, Crt, SecureCrt 等等都行。把设备的 Console 线连接至 SSL VPN 的 Console 端口，开启电源开关，通过终端软件就能观察到设备启动自检的过程。

设备启动后，系统自检到如下信息时：

```
Welcome to the initial configuration of your server!  
NOTE: Press 'y' if this is a stand-alone server or the first  
machine in a clustered configuration.  
If this is going to be a member of an already running cluster  
press n to reboot. When you see the 'Hit TAB for clustering options'  
message press TAB and follow the directions.  
Would you like to proceed (y/n)?: y (选择 Y)  
Note that continuing signifies that you accept the terms  
of the Neoteris license agreement. Type "r" to read the  
license agreement (the text is also available at any time  
from the License tab in the Administrator Console).  
Do you agree to the terms of the license agreement (y/n/r)?: y (选择 Y)
```

初始化网络信息：

```
Please provide ethernet configuration information  
IP address: 172.16.3.4  
Network mask: 255.255.255.0  
Default gateway: 172.16.3.254  
(填入用户需要的 IP 地址，掩码和网关等信息。  
注意：所有网络信息都会设置到 SSL VPN 的 Internal Interface 上)  
Link speed [Auto]:  
0) Auto  
1) 1000 Mb/s, Full Duplex  
2) 1000 Mb/s, Half Duplex  
3) 100 Mb/s, Full Duplex
```

- 4) 100 Mb/s, Half Duplex
- 5) 10 Mb/s, Full Duplex
- 6) 10 Mb/s, Half Duplex

Select 0-6: **0** (选择用户需要的速率)

Please provide DNS nameserver information:

Primary DNS server: 172.16.220.1

Secondary (optional): 172.16.3.2 (填入需设置的 DNS 地址, 可以是内部的 DNS 服务器)

DNS domain(s): bjsslvpn.cdhfund.com (填入需要的域名, 无特别限制)

Please provide Microsoft WINS server information:

WINS server (optional):

确认初始化信息:

Please confirm the following setup:

IP address: 172.16.3.4

Network mask: 255.255.255.0

Gateway IP: 172.16.3.254

Link speed: Auto

Primary DNS server: 172.16.220.1

Secondary DNS: 172.16.3.2

DNS domain(s): juniper.net

WINS server:

Correct? (y/n): **y** (确认无误后, 选择 Y)

初始化安全信息:

Admin username: **admin**

Password:

Confirm password:

The administrator was successfully created.

(填入用户设定的管理员帐号和密码, 这里输入的密码是不显示的)

设置 SSL VPN 自签证书:

Please provide information to create a self-signed Web server digital certificate.

Common name (example: secure.company.com): timerwell.juniper.net

Organization name (example: Company Inc.): juniper

(这个部分输入用户的证书信息, 无特殊限制)

Please enter some random characters to augment the system's random key generator. We recommend that you enter approximately thirty characters.

Random text (hit enter when done): dkfjlkjffieejjkdnfkkfjiiiffoerjooootpqe454646
(这个部分输入 30 个左右的字符以产生证书)

Creating self-signed digital certificate...

The self-signed digital certificate was successfully created.

Congratulations! You have successfully completed the initial set up of your server.
(当您看到这句话时证明你已经成功的初始化 **SSL VPN** 了)

`https://<IVE-IP-Address>/admin` (note the 's' in `https://`)

Example: `https://10.10.22.34/admin`

(按照上述的提示, 管理员就可以通过 URL `https:// 172.16.3.4/admin` 管理设备)

1.2、使用浏览器连接 SSL VPN

使用初始化时设置的管理员帐号及密码就可以登陆到 SSL VPN 进行管理了, 这里设置的用户名: admin 密码: dinghui@123



使用过程中可以根据需要更改用户名及密码或修改权限，如下图

[Auth Servers](#) > [Administrators](#) > [Update Administrator admin](#)

Update Administrator admin

Full Name:

Authenticate using: Administrators

Password:

Confirm Password:

☐ One-time use (disable account after the next successful sign-in)

☒ Allow console access

☒ Enabled

☐ Disabled

☐ Quarantined

☐ Require user to change password at next sign in

Note: You must also configure password management on the [Authentication server Settings](#) with 'Allow users to change their passwords' Password page to specify which realms should inherit the server's password management capabilities.

[Save Changes](#)


二、 SSL VPN 基本设置

2.1、网络接口更改

更改设备 IP 地址及网关，配置路径：Network → Internal Port

[Network](#) > [Internal](#) > [Internal Port - Settings](#)

Internal Port - Settings

 **Network Settings**
Internal Port - Settings

Overview **Internal Port** External Port Management Port VLANs Routes Hosts

[Settings](#) Virtual Ports ARP Cache ND Cache

Enter the network settings and click the Save Changes button at the bottom of the page.

IPV4 Settings

*IP Address:

*Netmask:

*Default Gateway:

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

DNS 地址: 172.16.220.1 & 172.16.3.2 配置路径: Network → Overview

Overview	Internal Port	External Port	Management Port	VLANs	Routes	Hosts
----------	---------------	---------------	-----------------	-------	--------	-------

Enter the network settings and click the Save Changes button at the bottom of the page.

▼ Status

Internal Port:	Connected, Speed: 100Mb/s, Duplex: full RxPacket: 9925404 RxError: 0 RxDrop: 0 TxPacket: 4688539 TxError: 0 TxDrop: 0
External Port:	Disabled
Management Port:	Disabled

▼ Network Identity

Hostname: Fully-qualified hostname

▼ DNS name resolution

Primary DNS: IP address

Secondary DNS: IP address

DNS Domain(s): Example: "company.com, company.net"

Note: If you need to resolve names without using DNS, you can do so on the [Hosts](#) page.

2.2、添加用户认证服务器

用户登入企业网须进行身份认证。在身份认证的过程中，管理员可以选择使用 SSL VPN 内部的自建帐号认证用户，也可以结合企业内部的认证服务器进行认证。对于选择不同的认证服务器的帐号，他们将会属于不同的 SSL VPN 认证域。

（说明：SSL VPN 内置两个认证服务器，Administrators 和 System Local，其中 Administrator 是添加 SSL VPN 管理员帐号的，而 System Local 是 SSL VPN 内建的一个普通用户的认证服务器；）

配置路径: Authentication → Auth. servers

新建 AD 认证服务器，配置路径：Auth. Servers → Authentication Servers

Settings

Users

Troubleshooting

▼ Base Configuration

* Name:

AD

Label to reference this server

* Domain:

CDHFUND

NetBIOS name of the domain

* Kerberos Realm:

CDHFUND.COM

Specifies the Kerberos realm of the Active Directory domain.
It is usually set to the DNS name of the Active Directory domain. Example "xyz.net", "abc.com"

▼ Domain Join Configuration

Username:

lw@cdhfund.com

Active Directory administrator credentials are required in order for the Pulse Connect Se

Password:

☒ Save credentials

If this setting is not enabled, the credentials entered will be destroyed after successfully

* Container Name:

computers

Container path in Active Directory to create the machine account in. Changing this field v

* Computer Name:

BJSSLVPN

Machine account name (do not include '\$')

在该页面上的 name 中输入认证服务器的名字等用户需要填入和勾选的其他选项，最后点击页面左下方“save changes”即完成新加一个认证服务器的设置了。

2.3、添加 SSL VPN 的认证域

SSL VPN 认证域的功能把不同的认证服务器加入到不同的域，来认证不同域上的用户，同时也方便用户了解自己登陆时应该选择哪一个认证域和哪一个认证帐号，避免出现帐号重复和认证混乱的局面。

新建认证域：CDH；认证方式：AD

配置路径：User Realms → New User Realm

General

Authentication Policy

Role Mapping

* Name:

CDH & CEPHEI

Description:

☐ When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

AD

User Directory/Attribute:

Same as above

Accounting:

None

Device Attributes:

None

在“name”中，填入认证域名。在“Authentication”中，选择使用“AD”认证服务器来认证用户，最后点击左下方“Save Changes”即完成了认证域的添加。

三、添加角色及角色映射

3.1、添加角色

在用户通过 SSL VPN 的身份验证之后，需要给用户分配角色，这个角色是在 SSL VPN 中设置的，并且这个角色决定了用户能够在企业内网中享有什么样的权限和能访问什么样的资源。

3.1.1 用户角色 CDH-Finance

配置路径: User Roles → New Roles

General
Web
Files
SAM
Telnet/SSH
Terminal Services

Overview
Restrictions
VLAN/Source IP
Session Options
UI Options

* Name:

Description:

[Save Changes](#)

Options

If these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used.

- ☐ VLAN/Source IP [\(Edit\)](#)
- ☒ Session Options [\(Edit\)](#)
- ☒ UI Options [\(Edit\)](#)
- ☐ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

角色的 Access features

Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- ☒ Web [0 Bookmarks | Options](#)
- ☐ Files, Windows [0 Bookmarks | Options](#)
- ☒ Files, UNIX/NFS [0 Bookmarks | Options](#)
- ☒ Telnet/SSH [0 Sessions | Options](#)
- ☐ Secure Application Manager [0 Applications | Options](#)
 - ☒ Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
 - ☐ Java version
- ☐ Terminal Services [0 Sessions | Options](#)
- ☐ Virtual Desktops [0 Sessions](#)
- ☐ HTML5 Access [0 Sessions | Options](#)
- ☐ Meetings [Options](#)
- ☐ VPN Tunneling [Options \(includes IKEv2\)](#)
- ☐ Secure Mail [Options](#)

[Save Changes](#)

* indicates required field