

## 15.11.2 Configuring VPN Access and Authentication

---

Click one of the buttons to take you to that part of the video.

Configuring VPN Access and Authentication 0:00-0:10

In this demonstration, we are going to show how to create an IPsec VPN.

---

Graphical Method 0:11-0:41

We do this from the graphical window. So, in this demonstration we're using Centos 7. You may need to choose something different with your distribution of Linux, but here what we do is we click on Applications and we go to System Tools.

In System Tools we go over to Settings and select.

In Settings we go over to Network and you can see here that VPN is not set up, so we'll go ahead and click on this + sign and we're going to create an 'IPsec based VPN'.

---

IPsec VPN 0:42-1:09

IPsec is more secure than in SSL VPN, so we'll go ahead and select that.

If the VPN that you're connecting to provides you with information, they may send it to you in the form of a configuration file, so you'll click here on import from file in that case.

We'll go ahead and click on IPsec based VPN.

---

VPN Name and General Information 1:10-2:23

We can name our VPN so, in this case we'll just name it TestOut.

Our Gateway, that is the IP address or the default name of the VPN you're connecting to. Let's just throw in an IP address of 192.168.10.10. Of course, that is an internal IP address, so it wouldn't work, but that's fine.

For the User Name, what is the user name you're logging in with, so we'll say testoutuser.

And then we specify the Group name. Now this is some of the information that you will be given from the VPN server.

You may need a User password. You may need to set a password. But if we click here on the question mark, it says that we can ask for this password every time. This is a good safety measure. This way, unauthorized users will probably be prevented.

We could go ahead and store the password for this user, for all users, or there may not be a password. That would be unlikely. But if we ask for the password every time, and we ask for the secret every time, then that puts the onus on the person who's trying to establish the VPN.

---

Advanced Settings 2:24-3:14

If we click here on Advanced, we can specify which algorithms we're going to use.

Again, this is very detailed and will be very specific to the VPN that you're connecting to. So, you might have different types of encryption like DES or AES or Triple DES.

For authentication, you might use MD5, or SHA-1, as an example. You might use different Diffie-Hellman groups like 1, 2, 5, or 14. There's many, many, many choices here, so that really is something you need to get from the VPN server.

The Domain as well. You might be logging into a domain, so you might need to put in the domain name of the system you're trying to log in to.

---

**IPv4 Settings 3:15-3:54**

Over here we can click on IPv4. Most of the time when you log into a VPN, they're going to provide you with an IP address. If not, you can go ahead and manually enter your IP address, by 192 168 100.1. Your Netmask and whatever your local Gateway is.

You can specify a DNS server. Typically, it will be automatic.

And you can put in Routes if you need to, but again, that will be automatic most of the time.

You could also disable IPv4, but again that would be unlikely.

---

**IPv6 Settings 3:55-4:11**

For IPv6 you can use whatever it is that you need to specify for IPv6. You might do automatic with DHCP. You might do a Link-local, whatever it is the system you're logging into requires.

Go ahead and click Add, and that's all there is to it.

---

**Saving Changes 4:09-4:21**

You now have the VPN.

You want to connect to it? You just flip that to On, connect to it, and it should then prompt you for your username and password.

---

**Summary 4:22-4:21**

In this demonstration, we showed how to create an IPsec VPN.

---

**Copyright © 2022 TestOut Corporation All rights reserved.**