Instructions for setting up a VPN site to site model on Cisco ASA systems

In the following article, we will show you some basic steps to set up and configure the site to VPN site with Cisco ASA system. Currently, the concepts and applications of VPN for users are many, typically include: site to site, remote access IPSec, client-less, SSL, DMVPN ... and will be very difficult to mention specifically to any one element ...

TipsMake.com - In the following article, we will present some basic steps to set up and configure site to VPN site mode with Cisco ASA system. Currently, the concepts and applications of VPN for users are many, typically include: site to site, remote access IPSec, client-less, SSL, DMVPN . and will be very difficult to mention specifically to any one component. Therefore, we will try to mention the most basic information and configuration steps, set up VPN, set up site to site VPN from CLI with specific description for each step. Besides, the method of setting up VPN via ASDM uses the VPN wizard extremely simple and easy. That is why we focus mainly on the CLI part.

Before we get started, let's take a look at some VPN related information. An acronym for **Virtual Private Network** , this is basically a connection from one location to another to form a LAN model with support services such as email, intranet . only accessible When the user correctly declared the information already set up. And in general, there are 2 types of popular VPN models today:

- **Remote access:** also known as **Remote access VPN** or **easy VPN** , for users with simple needs. The way to work is to just install the client software on your personal computer, PC or laptop, so that the user will establish a connection to the computer at the office, log in with the username and password parameters. previously assigned rights. After the tunnel has been replaced, the user can work and access the server directly as in the office, this tunnel connection protocol is built based on IPSec or SSL.

- **Site to site:** this system is often used between branches of an organization or a certain company network. Here, you must use a VPN-enabled device such as a Cisco ASA or Cisco router. Users can configure both devices to set up each other for tunneling systems, and all corporate or office models will be used over the tunnel at the same time (while VPN access connections are available). Remote can only be performed on the PC with the tunnel set up available) to access resources in the same system.

Tunnel setup is usually divided into two phases. Suppose, in our test, it will apply based on the following situation: in a company with 100 users, server system with LAN model to use for services like email, intranet, and history Using **Cisco ASA 5520 device** as an Internet gateway.

The address of the LAN here is **10.0.0.0/24** , the gateway parameter (ASA) has the internal address **10.0.0.254** and the outside is **1.1.1.1** . Currently, this company has opened more branches with 10 users, this office has 10 more personal computers and does not display any more servers, has Internet connection and uses ASA 5510 with the role of security. The LAN address of this office is **192.168.0.0/24** , gateway (ASA) with the internal IP

address of **192.168.0.254** , the outside is **1.1.1.2** .

Overview model of the network system

And the request from the management board is to want the computers at the branch to connect to the office via the site to site VPN model.

Begin:

Now is the time when we need to perform some setup operations, as follows:

- Frequently used addresses are initialized in the access list.

- This list will be accessed via **VPN** traffic from **NAT** protocol **(NAT0).**

- IPSec setup conversion mechanism will take on **IPSec** encryption tasks.

- The switching map system will initiate real **tunnels** for **IPSec** .

- **Isakmp** policy initializes the necessary settings for the request from the system in step 1.

- **Tunnel** groups set properties for **tunnel** .

To make sure the system works stably and there are no errors during the setup process, try to meet these requirements. Next is to check the NAT protocol and the list mentioned.

Interesting traffic:

One point to consider when creating VPN tunnels, you need to 'inform' ASA about the traffic sent through this tunnel - collectively referred to as **interesting traffic** , we can create this part using **access - list.** . On a site to site VPN system, users must set up both sides of the tunnel, and we must be careful when creating the corresponding **access - list** . Specifically, on the first site, ASA will receive a request from the system that tunnel traffic will be transferred from the main office to the branch. As for the other site, ASA will assume the opposite task, which is to transfer **tunnel traffic** from the branch to the headquarters.

The basic command structure is as follows:

access-list VPN_cryptomap extended permit ip 10.0.0.0 255.255.255.0 192.168.0.0 255.255.255.0

We can see that this list of **access - lists** is created on the main office, and is responsible for notifying ASA that traffic flows from address **10.0.0.0** to **192.168.0.0** will be added to the tunnel. All other **traffic** remaining will not be placed on this list, and continue the normal process by going straight through ASA. Next is the **access - list** section used at the branch:

access-list VPN_cryptomap extended permit ip 192.168.0.0 255.255.255.0 10.0.0.0 255.255.255.0

You should note once again that the way to move and select traffic is reversed with the special traffic, transmitted from the branch office to the headquarters in this case. The above is just a part of the basics of **interesting traffic** , the ASA system itself will select traffic based on users' options and allow to operate as usual. In addition, we will also have to initiate the corresponding actions and actions while setting up the conversion map mechanism.

NAT0:

Since directly connecting the network at the head office to the branch office, most of us do not need to perform the NAT process of the entire traffic flow between the above locations. If we want to set up some NAT models to connect to the Internet, we must ignore the traffic that needs to pass through the tunnel from NAT. To perform this step, we must use the **access - list** again:

access-list Inside_nat0_outbound extended permit ip 10.0.0.0 255.255.255.0 192.168.0.0 255.255.255.0

Similar to the interesting traffic sections that have been selected at this time. At the same time, we will also have to tell ASA what to do with the traffic that goes through here. In this case, you will have to create a new clause to do the NAT0 process - that is, do not perform NAT at this step:

nat (Inside) 0 access-list Inside_nat0_outbound

Note that here we use the NAT clause as usual to connect to the external console. After that, provide any number to initialize and define different parts of the tunnel, in this case we use zero to inform ASA that there is no need to use NAT protocol now. Here, we need to consult the list of **access - list that** has been initialized earlier.

Now, all traffic we choose in the access-list list will not have to go through NAT process through ASA anymore. And apply the same syntax as above for the branch system:

access-list Inside_nat0_outbound extended permit ip 192.168.0.0 255.255.255.0 10.0.0.0 255.255.255.0

nat (Inside) 0 access-list Inside_nat0_outbound

Note that we need to change the options to refer to the headquarters.

Next, this is a step that can be confusing to most of us, because the converter with the main function is to create and define the encryption mechanism of the system, or at the IPSec section. At this point, we have not implemented the encryption as described above. Both sides will discuss how to encode in different classes, and therefore need to be done together. For example, if you proceed with encryption with key A, you will have to decrypt the same key value, otherwise the user will not be able to read the contents of the message.

At this step, the administrator can initiate the function converter, but ASA is mostly built into these components. The basic syntax in this step is as follows:

crypto IPSec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto IPSec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto IPSec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto IPSec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

When you first look at this section of code, you may see redundancy and unnecessary, but one point to note is that the IPSec part of the conversion mechanism has been initialized by name.

Crypto map:

The next step is when we continue to create the necessary parts of the process to bring the tunnel into operation, grouping all the function blocks created in the previous step together - that is the **Crypto map.**

The first is the setup section that we will use on the main site, and then explain the individual functional parts:

crypto map VPN_map 10 match address VPN_cryptomap
crypto map VPN_map 10 set peer 1.1.1.2
crypto map VPN_map 10 set transform-set ESP-AES-256-SHA

The crypto map syntax is used first, and then the name part, followed by the setting number. The reason for these numbers is because we can only use crypto map on each interface. But this will be a problem if the user has two branch offices but only one part of the console.

But besides, Cisco has solved this problem by using Preference number. We can use the same crypto map on different parts of the interface, but we can use different **Preference** numbers on a tunnel. This way will help us set up and initialize many different tunnels on the same interface.

On the first command line, we will see the list of access - list created in the previous step, and this is also the way traffic is passed through the tunnel. Then the **peer** creation step - this is the rest of the tunnel, and in this case the branch office's WAN IP address.

Next, we will inform ASA about the encryption mechanisms that will be used at the IPSec layer. And once a crypto map is available after initialization, the component has not performed any functionality until it is applied to the interface. Here, make sure that it has been applied to the nearest tunnel interface layer, in this test the outside part is:

crypto map VPN_map interface outside

As for the branch office, we do the same, just change the WAN IP address parameters:

crypto map VPN_map 10 match address VPN_cryptomap
crypto map VPN_map 10 set peer 1.1.1.1
crypto map VPN_map 10 set transform-set ESP-AES-256-SHA
crypto map VPN_map1 interface

Isakmp Policy:

When this step is reached, the actual IPSec tunnel time is built, and the next thing to do is to build a security layer to manage and monitor traffic data streams - this is **Isakmp** or **phase 1.**

To create this **security** management class, you need to set up the necessary policies of ASA first:

crypto isakmp policy 10 authentication pre-share
crypto isakmp policy 10 encryption aes-256
crypto isakmp policy 10 hash sha
crypto isakmp policy 10 group 5
crypto isakmp policy 10 lifetime 86400

At this step, we must start each command line with **crypto isakmp policy** and then **Preference** number. The smaller these numbers are, the bigger the component will be configured, and the tunneling process will take place faster.

The first line of code in this process will indicate the basic part of the tunnel validation structure. Here, we can use **pre-share** or **certificate** keys, in which the pre-share key is the easiest to implement, and the certificate is often used in establishments and businesses with a large scope of operations.

Next is the definition of the encryption and validation mechanism, which looks quite similar to the above conversion, but is still used to encrypt data at the IPSec layer. Specifically, here our main task is to define the coding components, which were created before IPSec was established.

When we finish with setting and activating the operation mode of isakmp, ASA will switch to tunnel construction section:

crypto isakmp enable Outside

Tunnel groups:

Once this step has been completed, after we have completed the steps 1 and 2, we can use the tunnel - group to initialize the tunnel settings separately, in the tunnel of the site to site model. then we recommend that you use the IP address of **peers** as **group - name.** Our command syntax at this step is as follows:

tunnel-group 1.1.1.2 type ipsec-l2l
tunnel-group 1.1.1.2 IPSec-attributes
pre-shared-key testkey

Specifically, the first statement tells ASA that we are creating an IPSec tunnel. The second statement is used to refer to the previously initialized components: the pre - share key, we will set them up here and refer back to the policy section of crypto isakmp, and 1 more point to save. The idea is to create on both ASA models.

Generality:

When we have completed the above steps, we have successfully created tunnel site to site. Then, test on client machines using ping command, remote control or website access. Maybe we will fail in the first trial, but don't worry. But the first signal packet sent to ASA will take over the tunnel initialization task, and this process takes a while to complete. Try again, and we will get better results when 'seeing' all computers, printers, servers and other devices on both sides of the tunnel.

When you encounter any problems, you can use the following command:

show crypto isakmp sa
show crypto IPSec sa

The above syntax will show the results found if the tunnel is in the above steps on the signal response. Good luck!

You finished reading the article "**Instructions for setting up a VPN site to site model on Cisco ASA systems**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.