Configure Cisco ASA system with Android, VPN and Active Directory Authentication devices

In the following article, we will cover some basic operations to configure and set up Cisco ASA systems with devices based on Android, VPN operating system and Active Directory Authentication.

TipsMake.com - In the following article, we will present some basic actions to configure and set up Cisco ASA system with devices based on Android, VPN operating system and Active Directory Authentication. For example, how do you want to connect your HTC Incredible phone to the network of companies and offices to use and exploit smartphone utilities? Many have come up with ideas and methods but are not successful. But when the author of the article continued to persevere, search and test different options, they finally achieved the goal. Specifically, two smartphones HTC incredible 2.2 and Samsung Infuse have successfully connected to the network through the VPN model, although there are still some shortcomings.

Before embarking on the implementation and setup, we need to know that the ASA version of the iOS operating system must be 8.4.1 and Android 2.1 based on Cisco requirements. But in fact, there are some ASA models with only 512 MB of storage, so it is quite difficult and complicated to upgrade the iOS operating system.

Besides, if you are using the port service forward on the main external IP address, it will cause the system to stop working, because it does not support NAT in the VPN environment. If in this case, we will have 2 options:

- Delete the command line:

nat (outside, outside) dynamic source [name your VPN LAN] interface

This will prevent the VPN client components from accessing the Internet via VPN.

- Another way is to move the port component forward to another IP address.

Specifically, in this test we will apply on ASA 5505 system. On the other hand, if we want to implement **Active directory** integration process - should apply this method, it will need some form Radius server, the example here is NPS included in the **Windows Server 2008** operating system. Setting up and initializing the NPS server system is a completely different process, but quite simple and easy.

In the configuration commands below, we will use mostly ASA default syntax, you just need to replace the information inside the [] with its own data, * at the end of the line to note like and should not add any other parameters after the * symbol!

*ASA Version 8.4 (1) * Please make sure you have used the correct version?*
!
*hostname [name of asa hostname] * Example: MainASA*

names
!
Vlan1 interface
nameif inside
security-level 100
ip address [IP address of system asa local] 255.255.255.0
!
Vlan2 interface
nameif outside
security-level 0
ip address [IP OUTSIDE address] [external subnetmask]
!
Ethernet0 / 0 interface
switchport access vlan 2
!
*boot system disk0: /asa841-k8.bin * Make sure you are booting with version 8.4.1!*
same-security-traffic permit intra-interface
object network obj_any
subnet 0.0.0.0 0.0.0.0
*object network [system name lan1] * Example: MainLAN*
*subnet [subnet and mask of lan1] * For example: 192.168.1.0 255.255.255.0*
*object network [system name lan2] * This is optional if you have more than 1 connection to communicate*
subnet [lannet mask of lan2]
object network [name of lan3 system]
subnet [subnet and mask of lan3]
*object network [name of VPN LAN] * Example: VPN_NET*
*subnet [subnet and mask of VPN LAN] * Example: 172.16.30.0 255.255.255.0*
*object-group network [group name of spread systems] * Example: LANS*
network-object object [lan1 name]
network-object object [name lan2]
network-object object [lan3 name]
*ip local pool [IP address pool name] [IP Pool Range] mask [pool mask] * Example: GroupPool 172.16.30.5-172.16.30.200 255.255.255.0*
*nat (inside, outside) source static [lan group name] [lan group name] destination static [VPN LAN name] [name your VPN LAN] * Example: LANS LANS VPN_NET VPN_NET - NEW WAY OF DOING NONAT*
nat (outside, outside) source dynamic [name of VPN LAN] interface
!
object network obj_any
nat (inside, outside) dynamic interface
*route outside 0.0.0.0 0.0.0.0 [gateway address] 1 * Example: 199.10.199.10*
*route inside [subnet address and mask of lan1] [lan1 gateway address] 1 * Example: 10.0.0.0 255.0.0.0 10.61.0.1*
route inside [subnet address and mask of lan2] [lan2 gateway address] 1
route inside [subnet address and mask of lan3] [lan3 gateway address] 1
dynamic-access-policy-record DfltAccessPolicy
aaa-server TACACS + protocol tacacs +
AAA-RADIUS protocol radius server
*aaa-server [name of RADIUS] protocol radius server * Example: MainRAD*

*aaa-server [RADIUS server name] (inside) host [RADIUS server IP address] * Example: 10.1.2.1*
*key [radius key] * For example: secretsquirrel*
crypto ipsec ikev1 transform-set TRANS_ESP esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set TRANS_ESP_3DES_SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS_ESP_3DES_SHA transport mode
crypto ipsec ikev1 transform-set TRANS_ESP_ esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS_ESP_ mode transport
*crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5 TRANS_ESP_3DES_SHA TRANS_ESP_*
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto isakmp nat-traversal 21
crypto ikev1 enable outside
crypto ikev1 policy 10
pre-share authentication
encryption 3des
hash sha
2 group
lifetime 86400
group-policy DefaultRAGroup internal
group-policy DefaultRAGroup attributes
*dns-server value [ip address of your DNS server] * Example: 10.1.2.5*
vpn-tunnel-protocol l2tp-ipsec
DefaultRAGroup tunnel-group general-attributes
*address-pool [name of the pool address of VPN IP] * For example: GroupPool*
*authentication-server-group [RADIUS server name] * Example: MainRAD*
default-group-policy DefaultRAGroup
tunnel-group DefaultRAGroup ipsec-attributes
*ikev1 pre-shared-key [client pre-shared key] * For example: vpnpassword*
!

On Android devices, we open **Settings> Wireless and networks> VPN settings> Add VPN** , choose **L2TP / IPSec PSK VPN** . VPN name depends on the user, can be set to any information, set up external VPN server IP address, **IPSec PSK** configuration **(client pre-shared key)** was initialized in ASA, not activated **Secret** functions and need not to set up a domain search feature via DNS. Good luck!

following us regularly.