Allowing Microsoft PPTP through Cisco ASA

The Microsoft Point to Point Tunneling Protocol (PPTP) is used to create a Virtual Private Network (VPN) between a PPTP client and server. It is used for remote access from mobile users to connect back to their corporate network over the Internet. A PPTP client connects and authenticates to the PPTP server which assigns an IP address to the client and attaches the remote user to the network. After that, the remote user has full network connectivity just like being connected locally.

In the older PIX version 6.x, you could configure the PIX firewall itself to work as a PPTP server, thus you didn’t even need to have a Windows PPTP server in place. With the new ASA firewall however, you cannot terminate PPTP on the ASA itself. Therefore you must have a Microsoft PPTP server in the network in order to terminate PPTP connections from clients.

PPTP uses two protocols: GRE to encapsulate PPP packets and a control channel at TCP port 1723. Any stateful firewall would have a problem with allowing PPTP protocol without any special “fixup” because of the two protocols needed for communication (GRE and TCP 1723). Cisco ASA allows you to pass PPTP traffic through with a special “inspection” mechanism which checks the control traffic (TCP 1723) in order to dynamically open also access for GRE traffic to pass through with no problems.

In this post we will see two scenarios of allowing PPTP traffic through a Cisco ASA. In the first scenario we have a PPTP client on the inside of ASA which communicates with a PPTP server on the outside zone. In the second scenario we
have a PPTP client on the outside of ASA which communicates with a PPTP server on the inside.

Scenario 1: PPTP client on inside and server on outside

The first scenario above depicts a PPTP server located on the outside of the ASA (Internet) and PPTP clients on the inside. Using the “inspect” command in the global policy-map we can enable access from inside to outside for PPTP.
! enable Port Address Translation on the outside interface
ciscoasa(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0
ciscoasa(config)#global (outside) 1 interface

! Add PPTP inspection to the default policy-map using the default class-map
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect ptp

Scenario 2: PPTP client on outside and server on inside

This scenario depicts a PPTP server located on the inside network. Here we must configure static NAT for the PPTP server and allow the appropriate protocols from outside (GRE, TCP 1723)
! translate the PPTP server private address 192.168.1.1 to public 50.50.50.1
ciscoasa(config)# static (inside,outside) 50.50.50.1 192.168.1.1 netmask 255.255.255.255

! allow the appropriate protocols from outside to inside

ciscoasa(config)# access-list acl-out permit gre any host 50.50.50.1
ciscoasa(config)# access-list acl-out permit tcp any host 50.50.50.1 eq 1723
ciscoasa(config)# access-group acl-out in interface outside

About the Author

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books ("Cisco ASA Firewall Fundamentals" and "Cisco VPN Configuration Guide") which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blogs below:
http://www.networkstraining.com
http://www.tech21century.com