Continue

Let's set up a site-to-site VPN between the Branch Office and Headquarters using Cisco ASA firewalls, which can be configured in just 15 lines of code. If you already have another VPN tunnel, it may only require less than 10 lines. This guide assumes prior knowledge of Cisco ASA CLI syntax and site-to-site VPN fundamentals. Our goal is to establish a VPN connection between the Branch Office and Headquarters, allowing the client-pc (10.10.60.10) in the branch office to access the web server (192.168.10.10) in the headquarters. First, we need to configure the Cisco ASA non-VPN settings for the Branch Office: interface GigabitEthernet0/1 nameif USERS security-level 100 ip address 10.10.60.1 255.255.255.0 interface GigabitEthernet0/6 nameif OUTSIDE security-level 0 ip address 101.85.10.1 255.255.255.248 route OUTSIDE 0.0.0.0 0.0.0.0 101.85.10.6 1 object network ho-server-subnet subnet 192.168.10.0 255.255.255.0 object network user-subnet subnet 10.10.60.0 255.255.255.0 nat (USERS,OUTSIDE) dynamic interface Next, we need to enable IKEv1 on the outside interface and create an IKEv1 policy: Enable IKEv1 on the OUTSIDE interface crypto ikev1 enable OUTSIDE Create an IKEv1 policy with the desired algorithms and methods: crypto ikev1 policy 5 authentication pre-share encryption aes-256 hash sha group 5 lifetime 3600 Finally, we need to configure a tunnel-group and set the peer IP address: Create a tunnel-group and configure the peer IP address Please note that the pre-shared key (PSK) for the tunnel must be identical on both ends. Tunnel-group configuration is as follows: tunnel-group 201.85.10.1 type ipsec-l2l, and ipsec-attributes ikev1 pre-shared-key Cisco1234. Configure the Transform Set by combining security protocols and algorithms to protect VPN data, using crypto ipsec ikev1 transform-set AES-HMAC esp-aes-256 esp-sha-hmac 5. Next, configure a Crypto Map and apply it to the outside interface, which includes an ACL to identify traffic, peer IP, and IKEv1 transform-set created earlier. access-list BRANCH-TO-HO extended permit tcp object user-subnet object ho-server-subnet crypto map VPN-MAP 1 match address BRANCH-TO-HO crypto map VPN-MAP 1 set peer 201.85.10.1 crypto map VPN-MAP 1 set ikev1 transform-set AES-HMAC crypto map VPN-MAP 1 set security-association lifetime seconds 3600 It's optional to enable Perfect Forward Secrecy (PFS) for newly generated keys unrelated to previous ones. To prevent NAT, use the following command: nat (USERS,OUTSIDE) source static user-subnet user-subnet destination static ho-server-subnet ho-server-subnet. The configuration should be mirrored with identical Phase-1 and Phase-2 policies. crypto ikev1 enable OUTSIDE crypto ikev1 policy 5 authentication pre-share encryption aes-256 hash sha group 5 lifetime 3600 tunnel-group 101.85.10.1 type ipsec-l2l tunnel-group 101.85.10.1 ipsec-attributes ikev1 pre-shared-key Cisco123 crypto ipsec ikev1 transform-set AES-HMAC esp-aes-256 esp-sha-hmac access-list HO-TO-BRANCH extended permit tcp object ho-server-subnet object branch-user-subnet crypto map HQ-MAP 10 match address HO-TO-BRANCH crypto map HQ-MAP 10 set peer 101.85.10.1 crypto map HQ-MAP 10 set ikev1 transform-set AES-HMAC crypto map HQ-MAP 10 set security-association lifetime seconds 3600 crypto map HQ-MAP interface OUTSIDE nat (SERVERS,OUTSIDE) source static ho-server-subnet ho-server-subnet destination static branch-user-subnet branch-user-subnet To verify the status of phase-1 tunnels on an ASA, use the "show crypto isakmp sa" command. The output shows that the branch office ASA initiated the tunnel and uses IKEv1. For phase-2 IPSec tunnels, use the "show crypto ipsec sa" command to check the status. Monitoring "#pkts encrypt" and "#pkts decrypt" can help identify issues. If packets are encrypted but not decrypted, it's likely an issue with receiving packets on the other side. If packets are not being sent through the tunnel, it indicates a problem with local ASA configuration. To configure IKEv2 instead of IKEv1, follow these steps: 1. Disable IKEv1 configurations. 2. Enable IKEv2 on both sides using "crypto ikev2 enable OUTSIDE". 3. Define the IKEv2 policy using "crypto ikev2 policy 20" with AES-256 encryption and SHA-256 integrity. 4. Configure tunnel groups using "tunnel-group" commands, specifying IPsec-l2l as the protocol and the remote authentication method as pre-shared-key. 5. Create a crypto map to apply the IKEv2 policy using "crypto map VPN-MAP 1 match address BRANCH-TO-HO". Note: The only differences between IKEv1 and IKEv2 configurations are in the use of AES-256 encryption, SHA-256 integrity, and pre-shared-key authentication methods. Cisco ASA is configured for IKEv2 with pre-shared keys, however, many companies still use IKEv1 despite its unreliability & security concerns. IKEv2 uses only 4 messages to establish a tunnel compared to IKEv1's 9 or 6 in main and aggressive modes respectively. crypto ipsec ikev2 ipsec-proposal VPN-EXAMPLE protocol esp encryption aes-256 protocol esp integrity sha-256 crypto map VPN-MAP 1 match address HO-TO-BRANCH crypto map VPN-MAP 1 set peer 101.85.10.1 crypto map VPN-MAP 1 set ikev2 ipsec-proposal VPN-EXAMPLE crypto map VPN-MAP 1 set security-association lifetime seconds 3600 IKEv2 has several benefits, including fewer exchanged messages to establish a tunnel compared to IKEv1. Tunnel-group 101.85.10.1 type ipsec-l2l tunnel-group 101.85.10.1 ipsec-attributes ikev2 remote-authentication pre-shared-key Cisco123 ikev2 local-authentication pre-shared-key Cisco123 The configuration steps for a Cisco ASA to talk with a remote peer using IKEv2 include defining the encryption domain, specifying phase 1 policy, phase 2 proposal and connection profile. To configure and monitor a site-to-site VPN in ASDM, navigate to the "Configure" tab. Within this section, select "Site-To-Site VPN," then "Advanced," followed by "Crypto Maps." Here, you can specify the encryption settings for your VPN connection. The configuration involves several steps: defining the crypto map, matching addresses, setting peer IP addresses, and selecting transform sets. Additionally, you must set the security association lifetime in seconds. If this is the initial setup of a VPN, you will need to bind the crypto map to the interface facing the remote peers. In ASDM, once any VPN is configured, it automatically binds a crypto map to the selected interface. You can view these bindings under "Configure" > "Site-To-Site VPN" > "Connection Profiles." If this is your first IKEv2 setup, you will need to manually bind the crypto map and enable IKEv2 protocol on the specific interfaces facing the remote peers. This setting can be found in the connection profiles section of ASDM as well.

Cisco asa ikev2 vpn configuration. Cisco router ikev2 vpn configuration example. Cisco asa ikev2 configuration example. Cisco asa ikev2 ipsec vpn configuration. Cisco ikev2 vpn configuration. Cisco ios router ikev2 vpn configuration example. Cisco asa site to site vpn configuration example ikev2.