Palo alto ipsec vpn configuration guide

The IPSec tunnel configuration allows you to verify and/or encrypt the data (IP package) as it passes through the tunnel. If you set up the firewall to work with a peer that supports policy-based VPN, you need to define proxy IDs. Devices that support policy-based VPN use specific security rules/policies or access lists (source addresses, target addresses, and ports) to allow interesting traffic through an IPSec tunnel. These rules are mentioned during the rapid mode/IKE phase 2 negotiations and are exchanged as proxy IDs in the first or second message of the process. So if you're configuring the firewall to work with a policy-based VPN peer, you'll need to define the Proxy ID for a successful Phase 2 negotiation, so that the setting on both peers is identical. If the Proxy ID is not configured because the firewall supports router-based VPN, the default values used as Proxy ID are source IP: 0.0.0.0/0, destination ip: 0.0.0.0/0 and application: each; and when these values are exchanged with the peer, it results in a failure to set up the VPN connection. Select and then a new tunnel configuration. Enter a tunnel on the tab. Select which one you want to set the IPSec tunnel to. () Turn on IPv6 on the tunnel interface. Protect against a replay attack. () Save the type of service header for the priority or treatment of IP packages. () Select to enable GRE via IPSec.Enable Tunnel Monitoring.Create a Proxy ID to identify the VPN peers. If you set up site-to-site VPN: Make sure your Ethernet interfaces, virtual routers, and zones are configured correctly. For more information, see Configure Interfaces and Zones. Create your tunnel interfaces. Ideally, the tunnel interfaces will be placed in a separate zone, so that tunnelled traffic can use different policies. Set static routes or assign routing protocols to redirect traffic to the VPN tunnels. If you support dynamic routing (OSPF, BGP, RIP), you must assign an IP address to the tunnel interface. Define IKE gateways for establishing communication between peers across each end of the VPN tunnel; Also define the cryptographic profile that specifies the protocols and algorithms for identification, authentication, and encryption to be used to set up VPN tunnels in IKEv1 Phase 1. See Set up an IKE gateway and define IKE crypto profiles. Define security policies to filter and inspect traffic. If there is a refusal rule at the end of the security control base, traffic within the zone will be blocked unless otherwise allowed. Rules to allow IKE and IPSec applications must be explicitly above the are included. If your VPN traffic is going through (not coming or rising) a PA-7000 series or PA-5200 series FIREWALL, configure two-way security policies to allow ESP or AH traffic in both directions. When these tasks are completed, the tunnel is ready for use. Traffic intended for the defined in the policy is automatically redirected correctly based on the target route in the routing table and treated as VPN traffic. For a few examples on site-to-site VPN, see Site-to-Site VPN Quick Configs. To keep your business online and ensure that critical devices, such as Check Point firewalls, meet operational excellence standards, it's helpful to compare your environment with a third-party dataset. As part of the Indeni Automation Platform, customers have access to Indeni Insight, which benchmarks the acceptance of Check Point capabilities and user behavior to adhere to ITIL's best practices. +++ Overview: This document describes the step-by-step guide on configuring IPSec VPN and assumes that the Palo Alto Firewall has at least 2 interfaces in Layer 3 mode. If you find this article useful, see how to automate your PAN network with Indeni. High-level Diagram: IP Schema Specification: Steps to be tracked on Palo Alto Networks Firewall for IPSec VPN configuration Go to Network Interface &gt; Tunnel to create a new tunnel interface and assign the following parameters: Name: tunnel.1 Virtual router: By default, see this article if you need help configuring virtual router on Palo Alto networks. Zone: (select the internal zone layer 3 from which the traffic originates) See this article if you need help configuring the Layer 3 interface on Palo Alto Networks. Note: If the tunnel interface is in a different zone than the zone where traffic will originate or depart, a policy must be created to allow traffic to flow from the source zone to the tunnel interface zone. Configure IpSec Phase – 1 Configuration to Network Profiles &gt; Network Profiles &gt; IKE Crypto Profile and Define IKE Crypto (IKEv1 Phase-1) Parameters. (These parameters must match on the Cisco ASA firewall for the IKE Phase-1 negotiation to be successful) [divider width=full] Learn how indeni can enable preventive maintenance of your Palo Alto Networks Firewalls [divider width=full] Go to Network Profiles &gt; Network Profiles &gt; IKE Gateway to configure the IKE Phase-1 Gateway.; Note: The above tunnel ends in the traffic trust zone that crosses the tunnel, but if more detailed monitoring is required for the policy configuration in the tunnel, use a VPN or another zone. Also note that the gateway configuration below is configured for the Untrust interface, not to be confused with the tunnel that depends on a trusted interface. Under Network &gt; Network Profiles &gt; IPSec Crypto Profile, define the IPSec Crypto profile to create protocols and to provide identification, authentication and encryption in VPN tunnels based on IPSec SA negotiation (IKEv1 Phase-2). These parameters must match on the external firewall for the IKE Phase-2 negotiation to be successful. Note: DPD is a monitoring feature used to vibrancy of the Security SA (Security; Association and IKE, Phase 1) It is used to detect if the peer device still has a valid IKE-SA. Periodically, it will send an ISAKMP R-U-THERE package to the peer, which will respond back with an ISAKMP R-U-THERE-ACK confirmation. For more information about DPD, please refer this article. Related article Enlarging your team during difficult times configure IPSec Phase - 2 configuration Under Network &gt; IPSec Tunnel &gt; General, configure IPSec Tunnels to set the parameters to establish IPSec VPN tunnels between firewalls. Note: If Cisco ASA is configured as a policy-based VPN, enter the local proxy ID and external proxy ID that match the other side. When configuring an IPSec Tunnel Proxy ID configuration to identify local and external IP networks for traffic that is set, the Proxy ID configuration for the IPSec tunnel must be configured with post-NAT IP network data, because the Proxy ID information defines the networks allowed by the tunnel on both sides for the IPSec configuration. Note: By extending the View Advanced Options check box, there is an interesting feature that we can use, i.e. Tunnel Monitor. The Tunnel Monitor feature automatically initiates IPSec VPN Tunnel when the defined target IP address becomes accessible. In this example, 20.20.20.10 is the IP address configured on external site (behind Cisco ASA). PSec Tunnel Status The tunnel is not up, because on the other hand we have not configured the VPN yet. Under Network &gt; Virtual Routers &gt; Static Route, add a new route for the network behind the other VPN endpoint. Create the security policy to allow local network to communicate with remote network over the VPN. Capture the configuration. Here we are done configuring Palo Alto Firewall, now we can configure the Cisco ASA on the other side to successfully establish the IPSec VPN Tunnel. On Cisco ASA Firewall: Like Palo Alto Firewall, it also assumes that the Cisco ASA Firewall has at least 2 interfaces in Layer 3 mode. Configure IpSec phase – 1 on Cisco ASA Firewall. crypto ikev1 enable outside crypto ikev1 policy 10 authentication pre-share encryption aes hash sha group 2 lifetime 86400 ! !## ## ## ## Configure local and external network 10.10.10.0 255.255.255.0 ! ## Configureer ACL om VPN-verkeer bi-directioneel toe te staan !### access-list VPN-INTERESTING-TRAFIC extended permit ip object Cisco-Side object PA-Side nat (inside,outside) source static Cisco-Side Cisco-Side destination static PA-Side PA-Side no-proxy-arp route-lookup ! ! !Configure IPSec phase – 2 Policy !## ## ## tunnel group 1.1 1.1.1 type ipsec-l2l tunnel group 1.1.1.1 ipsec-attributes pre-shared-key 1234567 isakmp keepalive threshold 10 retry 2 ! crypto ipsec ikev1 transform-set VPN-TRANSFORM esp-aes esp-sha-hmac ! crypto map CRYPTO-MAP 1 match address VPN-INTERESTING-TRAFIC crypto map CRYPTO-MAP 1 set pfs group2 crypto map CRYPTO-MAP CRYPTO-MAP 1 set peer 1.1.1.1.1 crypto map CRYPTO-MAP 1 set ikev1 transform-set VPN-transform crypto-map CRYPTO-MAP interface outside Verify IPSec VPN Tunnel status of Cisco ASA Firewall, by pinging to one of the IP available address behind Palo Alto Firewall. ping 10.10.10.10 Send 5, 100-byte ICMP Echos to out PC, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms If and when we complete the IPSec VPN configuration on Cisco ASA Firewall as above, PA should display the following IPSec Tunnel Status. To validate tunnel monitor status in detail, log in to Palo Alto Firewall CLI and run the following command. Note that even if we didn't pass cisco ASA Firewall traffic through the VPN tunnel, Palo Alto Firewall would still show us the UP status for the IPSec VPN. The reason for this is that we have configured IPSec Tunnel Monitor on Palo Alto Firewall. When we configure IPSec Tunnel Monitor (as shown above), the destination IP address is examined by sending ICMP Echo Request, and when the response is received from the same IP address, the IPSec tunnel is up. &gt; vpn flow tunnel ID 1 tunnelPA Cisco_IPSEC id:1-type:IPSec gateway id:1 local ip:1.1.1.1 peer ip:2.2.2.2 inner interface:tunnel.1 1 outer interface:ethernet1/1 status:active session:6443 tunnel mtu:1436 lifespan:2663 sec last rekey:937 seconds ago monitor:on monitor status:up monitor interval:3 seconds monitor threshold:5 probe losses monitor packets sent:739180 monitor packets recv:732283 monitor packets seen:584 monitor packets reply:5 84 and/decap context:76 local spi:F18E58FF remote spi:B90FCFB2 In the output above: monitor packets sent – Number of monitor packets sent recv – Number of responses to the pings sent. Monitor Packets Response - Number of replies sent in response to monitor packets seen. This will only be increased if the requests are made to tunnel interface IP. Did you know that Indeni can continuously monitor the health of your Palo Alto Networks firewalls? Indeni gives you a heads-up when a firewall contract or certificate is about to expire by running these automation scripts: - Contract (s) about to expire Palo Alto Networks - Certificate(s) about to expire for Palo Alto Networks - Panorama certificate about to expire for Palo Alto Networks Want to know more about Indeni? Review our cisco solution and download our datasheet to see the latest supported Cisco versions. Darshan K. Doshi is a Security Consultant. He's been working with Palo Alto firewalls for about two years. If you also want to contribute, click here. Here.