

VPNaaS - Cisco ASA Firewall

Introduzione

Questa procedura è rivolta ai service provider/partner che vogliono attivare il servizio per se o per i propri clienti.

Di seguito i semplici passaggi di attivazione del servizio VPN su Public Cloud

Prerequisiti

Per realizzare la VPN occorre avere accesso al Firewall Cisco ASA in modalità "Privileged EXEC"

Guida passo-passo

1 Add IKE Policy

2 Add IPsec Policy

3

Sommario

- [Introduzione](#)
- [Prerequisiti](#)
- [Guida passo-passo](#)

Articoli collegati

Content by label

There is no content with the specified labels

Add VPN Service ✕

Name
 Create VPN service for current project.

Description
 The VPN service is attached to a router and references to endpoint group or a single subnet to push to a remote site. Specify a name, description, router, and subnet (optional) for the VPN service.

Router ⁺
 Admin State is enabled by default. The router and admin state fields require to be enabled. All others are optional.

Subnet [Ⓞ]
 Note: The recommended way to specify local subnets is to use endpoint groups in IPsec site connection. It is deprecated to specify subnet in VPN service. For a new VPN service or IPsec site connection, using endpoint group is recommended.

Enable Admin State [Ⓞ]

4 Add Endpoint Group ✕

Name
 Create endpoint group for current project.

Description

Type [Ⓞ]

Local System Subnets [Ⓞ]

- 192.168.168.0/24

5 Add Endpoint Group ✕

Name
 Create endpoint group for current project.

Description

Type [Ⓞ]

External System CIDRs [Ⓞ]

6 Add IPsec Site Connection ✕

Add IPsec Site Connection Optional Parameters

Name
 Create IPsec site connection for current project. Assign a name and a description for the IPsec site connection. All fields are required.

Description

VPN service associated with this connection ⁺

Endpoint group for local subnets [Ⓞ]

IPsec policy associated with this connection ⁺

IPsec policy associated with this connection ⁺

Peer gateway public IPv4 Address or FQDN [Ⓞ]

Peer router identity for authentication (Peer ID) [Ⓞ]

Endpoint group for remote peer [Ⓞ]

Peer key peer identifier [Ⓞ]

Pre-Shared Key (PSK) string [Ⓞ]

7 Configurazione Cisco ASA

```
ciscoasa> ena
Password: *****
ciscoasa#

ciscoasa# conf t
ciscoasa(config)#

! Inserire la Configurazione !
```

```
ciscoasa> ena
Password: *****
ciscoasa#

ciscoasa# conf t
ciscoasa(config)#

! Inserire la Configurazione !
```

CONFIGURAZIONE

```
object network NET_LOCAL
subnet $Local Subnet es: 192.168.52.0 255.255.255.0

object-group network NET_CLOUD
network-object $Remote Subnet es: 192.168.168.0 255.255.255.0

access-list VPN-CLOUD extended permit ip object NET_LOCAL object-group NET_CLOUD

nat (inside,Outside) source static NET_LOCAL NET_LOCAL destination static NET_CLOUD NET_CLOUD
no-proxy-arp route-lookup

crypto ipsec ikev1 transform-set esp-aes256-sha esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto ipsec df-bit clear-df Outside

crypto map CLOUD_MAP 10 match address VPN-CLOUD
crypto map CLOUD_MAP 10 set pfs
crypto map CLOUD_MAP 10 set peer $CLOUD IPv4 Address es: 185.132.70.13
crypto map CLOUD_MAP 10 set ikev1 transform-set esp-aes256-sha
crypto map CLOUD_MAP 10 set security-association lifetime seconds 86400
crypto map CLOUD_MAP interface Outside

crypto isakmp identity address
crypto ikev1 enable Outside

crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

NOTE:

\$Local Subnet = rete/i locale/i

\$Remote Subnet = rete/i remota/e

Configurazione testata con Cisco Adaptive Security Appliance Software Version 9.1(4)

SALVARE LA CONFIGURAZIONE:

```
ciscoasa(config)# end  
ciscoasa# write  
Building configuration...  
[OK]
```