

# VPNaaS - Sonicwall 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 Sonicwall in modalità "administrator"

## Guida passo-passo

## Configurazione Public Cloud

1 Add IKE Policy X

<p><b>Name</b> Policy_Name</p> <p><b>Description</b> Policy_Description</p> <p><b>Authorization algorithm</b> sha1</p> <p><b>Encryption algorithm</b> aes-256</p> <p><b>IKE version</b> v1</p> <p><b>Lifetime units for IKE keys</b> seconds</p> <p><b>Lifetime value for IKE keys</b> 3600</p> <p><b>Perfect Forward Secrecy</b> group2</p> <p><b>IKE Phase1 negotiation mode</b> main</p>	<p>Create IKE policy for current project. An IKE policy is an association of the following attributes:</p> <p><b>Authorization algorithm</b> Auth algorithm limited to SHA1 only.</p> <p><b>Encryption algorithm</b> The type of algorithm (bits, aes-128, aes-192, aes-256) used in the IKE policy.</p> <p><b>IKE version</b> The type of version (v1/v2) that needs to be filtered.</p> <p><b>Lifetime</b> Life time consists of unit and value. Units in 'seconds' and the default value is 3600.</p> <p><b>Perfect Forward Secrecy</b> PFS limited to using Diffie-Hellman groups 2, 5 (default) and 14.</p> <p><b>IKE Phase 1 negotiation mode</b> limited to main mode only.</p> <p>All fields are optional.</p>
---	--

Cancel **Add**

2 Add IPsec Policy X

<p><b>Name</b> IPsec_Policy_Name</p> <p><b>Description</b> IPsec_Policy_Description</p> <p><b>Authorization algorithm</b> sha1</p> <p><b>Encapsulation mode</b> tunnel</p> <p><b>Encryption algorithm</b> aes-256</p> <p><b>Lifetime units</b> seconds</p> <p><b>Lifetime value for IKE keys</b> 3600</p> <p><b>Perfect Forward Secrecy</b> group2</p> <p><b>Transform Protocol</b> esp</p>	<p>Create IPsec policy for current project. An IPsec policy is an association of the following attributes:</p> <p><b>Authorization algorithm</b> Auth algorithm limited to SHA1 only.</p> <p><b>Encapsulation mode</b> The type of IPsec tunnel (tunnel/transport) to be used.</p> <p><b>Encryption algorithm</b> The type of algorithm (bits, aes-128, aes-192, aes-256) used in the IPsec policy.</p> <p><b>Lifetime</b> Life time consists of unit and value. Units in 'seconds' and the default value is 3600.</p> <p><b>Perfect Forward Secrecy</b> PFS limited to using Diffie-Hellman groups 2, 5 (default) and 14.</p> <p><b>Transform Protocol</b> The type of protocol (esp, ah, ah+esp) used in IPsec policy.</p> <p>All fields are optional.</p>
---	--

Cancel **Add**

3

### Sommario

- [Introduzione](#)
- [Prerequisiti](#)
- [Guida passo-passo](#)
- [Configurazione Public Cloud](#)
- [Configurazione Sonicwall](#)

### Articoli collegati

- [VPNaaS - Sonicwall Firewall](#)
- [Deploy Sophos Firewall su Public Cloud](#)
- [Creazione Istanza \(VM\)](#)
- [Cloud-Init, utente con password e configurazioni aggiuntive.](#)
- [Quickstart Panoramica Public Cloud](#)

### Add VPN Service ✕

**Name** Create VPN service for current project.

VPN\_Service\_Name

**Description** The VPN service is attached to a router and references to endpoint group or a single subnet to push to a remote site.

VPN\_Service\_Description

**Router** Specify a name, description, router, and subnet (optional) for the VPN service.

test

**Subnet** Admin State is enabled by default.

192.168.168.0/24 The router and admin state fields require to be enabled. All others are optional.

**Enable Admin State**

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.

Cancel Add

### 4 Add Endpoint Group ✕

**Name** Create endpoint group for current project.

NET\_LOCAL

**Description**

**Type**

Subnet (for local systems)

**Local System Subnets**

- 192.168.168.0/24

Cancel Add

### 5 Add Endpoint Group ✕

**Name** Create endpoint group for current project.

NET\_REMOTE

**Description**

**Type**

CIDR (for external systems)

**External System CIDRs**

192.168.52.0/24

Cancel Add

### 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.

IPsec\_Site

**Description**

IPsec\_Description

**VPN service associated with this connection**

VPN\_SVC

**Endpoint group for local subnets**

NET\_LOCAL

**IPsec policy associated with this connection**

IPsec\_P1

**IPsec policy associated with this connection**

IPsec\_P2

**Peer gateway public IPv4 Address or FQDN**

peer IPv4 Address es 1.1.1.1

**Peer router identity for authentication (Peer ID)**

peer IPv4 Address es 1.1.1.1

**Endpoint group for remote peer (Peer ID)**

NET\_REMOTE

**Peer key peer identifier**

192.168.52.0/24 private. No owner for this resource

**Pre-Shared Key (PSK) string**

.....

Cancel Add

## Configurazione Sonicwall

1 SONICWALL™ Network Security Appliance

General Network Proposals Advanced

Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name: VPN-SERVER-CORTEX

IPsec Primary Gateway Name or Address: 185.132.70.80

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Shared Secret: [REDACTED]

Confirm Shared Secret: [REDACTED]  Wash Shared Secret

Local IKE ID: [IPv4 Address] 185.214.2.2

Peer IKE ID: [IPv4 Address] 172.16.51.254

Ready

OK CANCEL HELP

2 SONICWALL™ Network Security Appliance

Name: NET\_SERVER\_CORTEX

Zone Assignment: VPN

Type: Network

Network: 172.16.50.0

Netmask/Prefix Length: 255.255.255.0

Ready

OK CANCEL

NOTE: Nella sezione Remote Networks l'oggetto selezionato deve appartenere alla zona VPN !

3 SONICWALL™ Network Security Appliance

General Network Proposals Advanced

Local Networks

Choose local network from list: 10.172 Subnet

Local network obtains IP addresses using DHCP through this VPN Tunnel

Any address\*

Remote Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Choose destination network from list: NET\_SERVER\_CORTEX

Ready

OK CANCEL HELP

4

SONICWALL Network Security Appliance

General Network **Proposals** Advanced

### IKE (Phase 1) Proposal

Exchange: Main Profile  
 DH Group: Group 2  
 Encryption: 3DES  
 Authentication: SHA1  
 Life Time (seconds): 28800

### Ipssec (Phase 2) Proposal

Protocol: ESP  
 Encryption: 3DES  
 Authentication: SHA1  
 Enable Perfect Forward Secrecy  
 Life Time (seconds): 28800

Ready

OK CANCEL HELP

5 SONICWALL Network Security Appliance

General Network Proposals **Advanced**

### Advanced Settings

Enable Keep Alive  
 Suppress automatic Access Rules creation for VPN Policy  
 Disable IPSec Anti-Replay  
 Require authentication of VPN clients by XAUTH  
 Enable Windows Networking (NetBIOS) Broadcast  
 Enable Multicast  
 Permit Acceleration  
 Display Suite B Compliant Algorithms Only  
 Apply NAT Policies  
 Allow SamePathN Level 3 Management

Management via the SA:  HTTPS  SSH  SNMP  
 User login via the SA:  HTTP  HTTPS  
 Default LAN Gateway (optional): 0.0.0.0  
 VPN Policy bound to: Zone WAN

Ready

OK CANCEL HELP

Spuntare Enable keepalive

6

SONICWALL Network Security Appliance

General **Advanced** IPS IPS

### Settings

Name: Conf\_CIPMG  
 Action:  Allow  Deny  Discard  
 Type: VPN  
 In: 3DES  
 Service/Port: Any  
 Service: Any  
 Source: VPN\_Certifi\_Network  
 Destination: Any  
 SDOCS Protocol: All  
 Drop Disabled: None  
 Schedule: Always on  
 Priority: Retain original priority  
 Enable Logging  Enable Default Filter  
 Allow Fragmented Packets  Enable UDP Transformation

Ready

OK CANCEL HELP

NOTE: La zona di destinazione DEVE essere l'interfaccia specifica !  
non utilizzare la zona se è associata a più interfacce