

WebAdmin - U x Sophos User E x Symbols of Po x meaning of kabl x (27 unread) x Continuous Bil x Sophos Knowl x

https://10.8.8.2:4444

SOPHOS UTM 9 | admin | ? C

search IPsec

Dashboard Management Definitions & Users Interfaces & Routing Network Services Network Protection Web Protection Email Protection Endpoint Protection Wireless Protection Webserver Protection RED Management Site-to-site VPN Amazon VPC IPsec SSL Certificate Management Remote Access Logging & Reporting Support Log off

Connections Remote Gatew... Policies Local RSA Key Advanced Debug

+ New IPsec policy...

Display: 10 1-9 of 9

**Edit IPsec policy**

Name: MISSIONMED

IKE encryption algorithm: AES 256

IKE authentication algorithm: SHA1

IKE SA lifetime: 28800

IKE DH group: Group 2: MODP 1024

IPsec encryption algorithm: DES

IPsec authentication algorithm: SHA1

IPsec SA lifetime: 3600

IPsec PFS group: Group 2: MODP 1024

Strict policy: ☐

Compression: ☐

Comment:

Save Cancel

**Action**

Name
IPsec Settings: AES 128 / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<b>AES-256</b>
Compression off, not using strict policy.
IKE Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds
IPsec Settings: AES 256 / MD5 / Null (None) Lifetime: 3600 seconds
<b>AES-256 PFS</b>
Compression off, not using strict policy.
IKE Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds
IPsec Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<b>Microsoft Windows</b>
Compression off, not using strict policy.

WebAdmin - U x Sophos User E x Symbols of Po x meaning of kabl x (27 unread) x Continuous Bil x Sophos Knowl x

https://10.8.8.2:4444

SOPHOS UTM 9 | admin | ? C

search IPsec

Dashboard Management Definitions & Users Interfaces & Routing Network Services Network Protection Web Protection Email Protection Endpoint Protection Wireless Protection Webserver Protection RED Management Site-to-site VPN Amazon VPC IPsec SSL Certificate Management Remote Access Logging & Reporting Support Log off

Connections Remote Gatew... Policies Local RSA Key Advanced Debug

+ New Remote Gateway...

Display: 10 1-1 of 1

**Edit Remote Gateway**

Name: VPN-MISSIONMED

Gateway type: Initiate connection

Gateway: REMOTE GW

Authentication type: Preshared key

Key: \*\*\*\*\*

Repeat: \*\*\*\*\*

VPN ID type: Hostname

VPN ID: MMB-FIREWALL

Remote Networks:

PACMED NETWORK

DND DND DND DND

Comment: From Delia's Home to Office

Advanced

**Action**

Name	Host	Authen...
<b>VPN-MISSIONMED</b>	REMOTE GW MISSIONMED	
VPN ID is Hostname [MMB-FIREWALL], authenticated via Preshared key.		
From Delia's Home to Office		

WebAdmin - U...Sophos User E...Symbols of Po...meanig of kabi... (27 unread) -...Continuous Bil...Sophos Knowl...

https://10.8.8.2:4444

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

SOPHOSUTM 9

admin

searchIPsec

Dashboard

Management

Definitions & Users

Interfaces & Routing

Network Services

Network Protection

Web Protection

Email Protection

Endpoint Protection

Wireless Protection

Webserver Protection

RED Management

Site-to-site VPN

Amazon VPC

IPsec

SSL

Certificate Management

Remote Access

Logging & Reporting

Support

Log off

ConnectionsRemote Gatew...PoliciesLocal RSA KeyAdvancedDebug

New IPsec connection...

Open live log

Display: 101-1 of 1

Edit IPsec connection

Name: HOME-TO-OFFICE

Remote Gateway: VPN-MISSIONMED

Local Interface: WAN

Policy: MISSIONMED

Local Networks

TEST NETWORK

DND DND DND

DND DND DND

DND DND DND

DND DND DND

☐ Automatic Firewall Rules

☐ Strict Routing

☐ Bind Tunnel to Local Interface

Comment:

ActionStatusNameInterfacePolicyGateway

EditDeleteClone

HOME-TO-OFFICE

WAN

VPN-MISSIONMED

MISSIONMED

[Auto Firewall is off and strict routing is not in use.]

WebAdmin x Sophos Use x Web Mana x Symbols of x meaning of x (27 unread x Continuous x Sophos Knc x

https://pacmed.dyndns.org:1111/gateway\_to\_gateway.htm#1

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

LINKSYS  
A Division of Cisco Systems, Inc.

Firmware Version: 1.3.12.19-tm

VPN

10/100 4-port VPN Router RV042

System Summary

Setup

DHCP

System Management

Port Management

Firewall

ProtectLink

VPN

Log

Wizard

Support

Logout

Summary | Gateway to Gateway | Client to Gateway | VPN Client Access | VPN Pass Through | PPTP Server

Edit the Tunnel

Tunnel No. 3

Tunnel Name MMB-FW

Interface vWAN1

Enable ☒

Local Group Setup

Local Security Gateway Type IP Only

IP address 89 . 199 . 149 . 114

Local Security Group Type Subnet

IP address 192 . 168 . 1 . 0

Subnet Mask 255 . 255 . 255 . 0

Remote Group Setup

Remote Security Gateway Type IP Only

IP by DNS Resolved 0

Remote Security Group Type Subnet

IP address 10 . 8 . 8 . 0

Subnet Mask 255 . 255 . 255 . 0

IPSec Setup

Keying Mode IKE with Preshared key

Phase1 DH Group Group2

Phase1 Encryption AES-256

Phase1 Authentication SHA1

Phase1 SA Life Time 28800 seconds

Perfect Forward Secrecy ☒

Phase2 DH Group Group2

Phase2 Encryption AES-256

Phase2 Authentication SHA1

Phase2 SA Life Time 3600 seconds

Preshared Key @ELSHADDAI07@

Advanced -

Advanced

☒ Aggressive Mode

☒ Compress (Support IP Payload Compression Protocol(IPComp))

☐ Keep-Alive

☒ AH Hash Algorithm SHA1

☒ NetBIOS broadcast

☐ NAT Traversal

☐ Dead Peer Detection (DPD) Interval 60 seconds

Save Settings

Cancel Changes

SITEMAP

By setting this page, users can add the new tunnel between two VPN devices.

Tunnel No.: The tunnel number will be generated automatically from 1-50.

Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc.

More...

CISCO SYSTEMS