



# Getting Started with IPsec Site-to-Site VPNs on Sophos Firewall

**Sophos Firewall**  
Version: 19.0v1

## IPsec Site-to-Site VPNs

### Route-based VPN

- VPN connection is independent of routes for traffic
- Routes can be modified without disconnecting VPN
- Routes are created manually

### Policy-based VPN

- Local and remote networks are defined as part of the VPN
- VPN must be edited to change networks and requires disconnecting and reconnecting
- Routes are created automatically

SOPHOS

O Sophos Firewall suporta dois tipos de VPN IPsec; baseado em rotas e em políticas. Com VPNs baseadas em rota, você cria uma conexão VPN entre dois firewalls e, em seguida, configura separadamente o roteamento para o tráfego que deseja enviar pela conexão.

Com VPNs baseadas em políticas, você define as redes locais e remotas como parte da conexão VPN e as rotas serão criadas apenas para essas redes.

A vantagem das VPNs baseadas em rota é que você pode fazer alterações no tráfego que está sendo roteado a conexão sem ter que editar e, portanto, desconectar e reconectar a VPN.

# IPsec VPN Profiles

IPsec VPN profiles are configured in:  
**SYSTEM > Profiles > IPsec profiles**



Parâmetros de segurança usados para estabelecer e manter a conexão VPN



Ambos os lados da VPN devem permitir as mesmas configurações



Existem vários perfis fornecidos prontos para uso

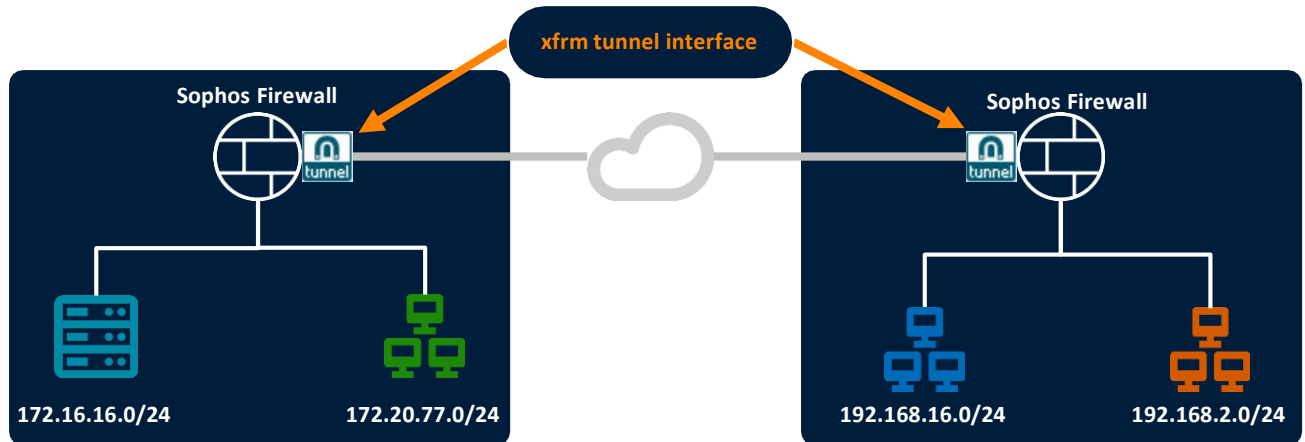
<input type="checkbox"/>	Default Profile	Automatic	Main mode	No	Enable	AES256 - SHA2 256	AES256 - SHA2 256	
<input type="checkbox"/>	DefaultBranchOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
<input type="checkbox"/>	DefaultHeadOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
<input type="checkbox"/>	DefaultL2TP	Automatic	Main mode	Yes	Disable	3DES - SHA1 3DES - MD5 AES128 - MD5	3DES - SHA1 3DES - MD5 AES128 - MD5	
<input type="checkbox"/>	DefaultRemoteAccess	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	
<input type="checkbox"/>	IKEx2	Automatic	Main mode	No	Enable	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	
<input type="checkbox"/>	Microsoft Azure	Automatic	Main mode	No	Disable	AES256 - SHA2 256 AES256 - SHA2 512	AES256 - SHA2 512 AES256 - SHA2 256	

SOPHOS

As VPNs IPsec exigem um conjunto correspondente de algoritmos e configurações em ambas as extremidades para que um túnel seja criado com êxito. No Sophos Firewall, eles são configurados em perfis IPsec.

Existem vários perfis pré-configurados que acompanham o Sophos Firewall, mas eles podem ser clonados e modificados para atender às suas necessidades. Isso pode ser necessário para atender aos critérios de conformidade ou para criar uma VPN com um dispositivo de terceiros.

## Route-Based VPN



SOPHOS

Quando você cria uma VPN baseada em rota, uma interface de túnel xfrm é criada no Sophos Firewall. Isso pode ser configurado como qualquer outra interface, exceto que está sempre na zona VPN. Você pode criar rotas, regras NAT e regras de firewall da mesma forma que faria para qualquer outro tráfego.

# Creating the VPN Tunnel Interfaces

IPsec VPNs are configured in:  
**CONFIGURE > Site-to-Site VPN > IPsec**

**General settings**

Name: NewYork

IP version: ☐ IPv4 ☐ IPv6 ☒ Dual

Activate on save ☐ Create firewall rule ☐

Description: Description

Connection type: Tunnel interface

Gateway type: Initiate the connection ☒

**Encryption**

Profile: IKEv2

Authentication type: Preshared key

Preshared key: .....

SOPHOS

Vejamos como você pode configurar isso. Examinaremos a configuração de um lado do túnel; no entanto, isso terá de ser feito em ambas as extremidades.

O primeiro passo é criar as interfaces de túnel. Isso é feito criando uma nova configuração IPsec; selecione Interface de túnel para o tipo de conexão.

Você notará que, ao selecionar a interface do túnel, a versão do IP muda automaticamente para Dual, pois as interfaces de túnel oferecem suporte a IPv4 e IPv6.

Um lado da conexão deve ser configurado para iniciar a conexão. O outro pode ser configurado para responder apenas.

Na seção 'Criptografia', selecione o perfil IPsec e o tipo de autenticação que deseja usar.

## Creating the VPN Tunnel Interfaces

Gateway settings

Local gateway	Remote gateway
<p>Listening interface</p> <p>PortB - 192.168.0.242 ✓</p>	<p>Gateway address</p> <p>192.168.0.228 ✓</p>
<p>Local ID type</p> <p>Select local ID ✓</p>	<p>Remote ID type</p> <p>Select remote ID ✓</p>
<p>Local ID</p> <p>✓</p>	<p>Remote ID</p> <p>✓</p>
<p>Local subnet</p> <p>Add new item</p>	<p>Remote subnet</p> <p>Add new item</p>
<p><input type="checkbox"/> Network Address Translation (NAT) You must first create these subnets in "Hosts and services".</p>	

You can configure the local and remote subnets if you select IPv4 or IPv6.







You do not need to specify the local and remote networks for tunnel interfaces

SOPHOS

Na seção "Configurações do gateway", selecione a interface local que será usada para criar a VPN e digite o endereço IP do firewall que estará do outro lado.

Ao configurar os gateways locais e remotos, você não especifica as redes locais e remotas para interfaces de túnel; no entanto, você deve definir o endereço do gateway remoto. Ao contrário das VPNs IPsec, você não pode usar um curinga para o endereço do gateway remoto, mesmo que a interface do túnel esteja configurada para responder somente.

# Configuring the Tunnel Interfaces

 <b>PortB</b> WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.0.242/255.255.255.0 DHCP 192.168.0.250/255.255.255.0 (PortB:0)	Hardware: PortB	 	
 <b>PortD</b> DMZ Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	172.30.30.16/255.255.255.0 Static	Hardware: PortD		

### General settings

Name \*

xfrm1

Hardware

xfrm1

IPsec connection

NewYork

Network zone

VPN

☒ IPv4 configuration

IPv4/netmask \*

172.18.254.1

/24 (255.255.255.0)

Tunnel interfaces are always in the VPN zone

**SOPHOS**

Depois de salvar a conexão IPsec, você verá que uma nova interface foi criada para ela. O será vinculada à interface física selecionada quando você criou a conexão IPsec.

A interface em si é configurada da mesma forma que qualquer outra interface; no entanto, você não pode configurar a região. As interfaces de túnel estão sempre na zona VPN.

Você deve garantir que as interfaces de túnel em cada extremidade do túnel estejam na mesma sub-rede.

# Routing for Route-Based VPNs

Configure routes to send the traffic over the tunnel  
Supports **static routes**, **SD-WAN policy routes**, and **dynamic routing**

**SOPHOS** Firewall

Feedback | How-to guides | Log viewer | Help | admin@fw1.ad.trainingdemo.xyz | Sophos

Search

MONITOR & ANALYZE  
Control center  
Current activities  
Reports  
Zero-day protection  
Diagnostics

PROTECT  
Rules and policies  
Intrusion prevention  
Web  
Applications  
Wireless  
Email  
Web server  
Advanced protection

CONFIGURE  
Remote access VPN  
Site-to-site VPN  
Network  
**Routing**  
Authentication  
System services

## Routing

SD-WAN routes | SD-WAN profiles | Gateways | Static routes | BGP | OSPF | Information

Current precedence for routing: Static route, SD-WAN route, VPN route.  
Policy route also applies to system-generated and reply traffic. To learn how to change the configuration, go to the [online help](#).

IPv4 | IPv6

IPv4 SD-WAN route | Watch: How to use SD-WAN routes

	#	Name	Interface	Source	Destination	Services	Application	ID	Active
	1	NewYorkIpsec in 0 B, out 0 B	Any	Any	US LAN	Any service	Any application	#1	<span style="color: green;">●</span>

Add | Delete

Depois de configurar as interfaces de túnel, você pode criar rotas para que o tráfego use o VPN. O roteamento pode ser configurado usando rotas estáticas, rotas de política SD-WAN e roteamento dinâmico.



## Simulação: Criar uma VPN site a site IPsec baseada em rota



Nesta simulação, você criará uma VPN site a site IPsec baseada em rota entre dois Firewalls Sophos.

LAUNCH SIMULATION


CONTINUE

<https://training.sophos.com/fw/simulation/IpsecVpnS2s/1/start.html>

SOPHOS

Nesta simulação, você criará uma VPN site a site IPsec baseada em rota entre dois Sophos Firewalls.

# Policy-Based IPsec VPN: IPsec VPN Wizard

 VPN connection wizard

Local server will allow you to select the WAN port, which acts as the endpoint for your tunnel

Local subnet will allow you to select the local network(s) you want to give access to remote users via this connection



For preshared key and RSA key, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable

For local certificate, ID and its value configured in "Local certificate" is displayed automatically


### Local network details

Local WAN port \*

IP version \* ☒ IPv4 ☐ IPv6

Local subnet \*   

Local ID



Site To Site

SOPHOS

Agora veremos a configuração de VPNs baseadas em políticas.

Há um assistente que pode ser iniciado a partir da página VPN site a site IPsec, que pode ser usado para criar uma VPN baseada em política. O assistente percorrerá as etapas necessárias para criar uma VPN, fornecendo ajuda e descrições adicionais para cada campo à esquerda.

# Policy-Based IPsec VPN



General settings

Name

NewYork

Description

Description

IP version

☒ IPv4 ☐ IPv6 ☐ Dual

Connection type

Site-to-site

Gateway type

Respond only

☐ Activate on save

☐ Create firewall rule

SOPHOS

Vamos percorrer a configuração criada pelo assistente.

Nas 'Configurações gerais' você pode escolher entre IPv4 ou IPv6 e se o Sophos Firewall deve responder apenas a solicitações VPN ou tentar iniciá-las.

Quando você está criando uma nova VPN, você também pode, opcionalmente, optar por fazer com que o Sophos Firewall crie automaticamente regras de firewall, embora elas sejam bastante gerais e devam ser revisadas.

# Policy-Based IPsec VPN

2

Encryption

Profile: IKEv2

Authentication type: RSA key

Local RSA key

Remote RSA key

Copy this to the 'Remote RSA key' field on the peer device

Copy this from the 'Local RSA key' field on the peer device

SOPHOS

Na seção "Criptografia", você seleciona o perfil VPN, um dos perfis prontos para uso ou um que você mesmo criou. Selecione o tipo de autenticação, que pode ser uma chave pré-compartilhada, uma chave RSA ou um certificado digital.

As chaves pré-compartilhadas são uma senha inserida em ambos os dispositivos. Esse geralmente é o tipo de autenticação mais fraco, principalmente porque o comprimento da chave geralmente é curto em comparação com as outras opções.

As chaves RSA são pares de chaves privadas públicas. A chave pública é copiada de cada dispositivo para o outro dispositivo. Isso fornece boa segurança, pois o comprimento da chave é muito maior e chaves diferentes são usadas para cada dispositivo. Como bônus, você não precisa criar uma senha, você pode simplesmente copiar e colar as chaves.

Os certificados digitais são a opção mais segura, mas exigem algum esforço adicional para configurar. Eles fornecem pares de chaves privadas públicas semelhantes às chaves RSA, mas também são assinados por autoridades de certificação confiáveis e têm os comprimentos de chave mais longos.

# Policy-Based IPsec VPN



Gateway settings

Local gateway

Listening interface

PortB - 192.168.0.242

Local ID type

DNS

Local ID

fw1.trainingdemo.xyz

Local subnet

UK LAN

Add new item

Remote gateway

Gateway address

\*

Remote ID type

DNS

Remote ID

fw2.trainingdemo.xyz

Remote subnet

US LAN

Add new item

☐ Network Address Translation (NAT)  
You must first create these subnets in "Hosts and services".

SOPHOS

Nas "Configurações do gateway", você configura a interface que o Sophos Firewall usará para a VPN e onde ela se conectará. Se o lado remoto tiver um endereço IP dinâmico, um curinga pode ser usado; no entanto, isso também significa que o Sophos Firewall não pode iniciar a conexão, pois não sabe para onde se conectar.

As VPNs IPsec também podem ter um ID, que pode ser baseado em DNS, endereço IP, endereço de e-mail ou um nome de certificado X.509.

Finalmente, você precisa definir quais redes estarão disponíveis através da VPN. Ou seja, as redes locais que os dispositivos remotos poderão acessar e as redes remotas que você espera poder acessar pela VPN.

## IPsec Acceleration

```
console> system ipsec-acceleration disable
```

This will restart all IPsec tunnels and stop offloading IPsec VPN traffic to the Xstream flow processor.

Turn off IPsec acceleration(Y/N)?

Y

```
console> system ipsec-acceleration enable
```

This will restart all IPsec tunnels and offload IPsec VPN traffic to the Xstream flow processor.

Turn on IPsec acceleration(Y/N)?

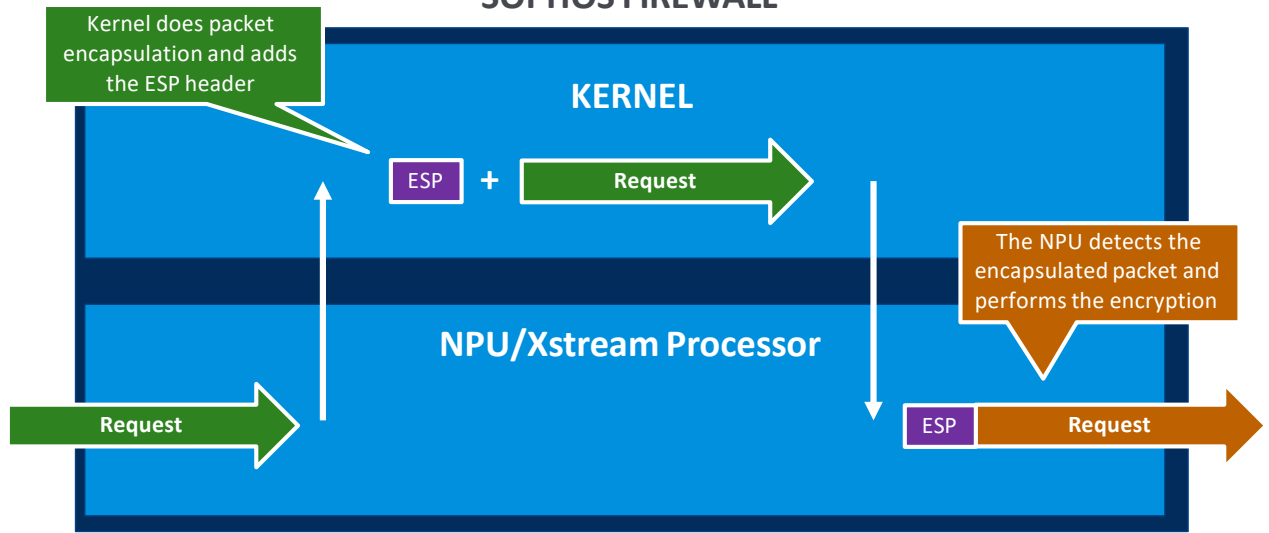
Y

### SOPHOS

A aceleração IPsec é configurada no Console usando o comando `system ipsec-acceleration` para ativar e desativar o recurso.

# IPsec Acceleration

## SOPHOS FIREWALL



SOPHOS

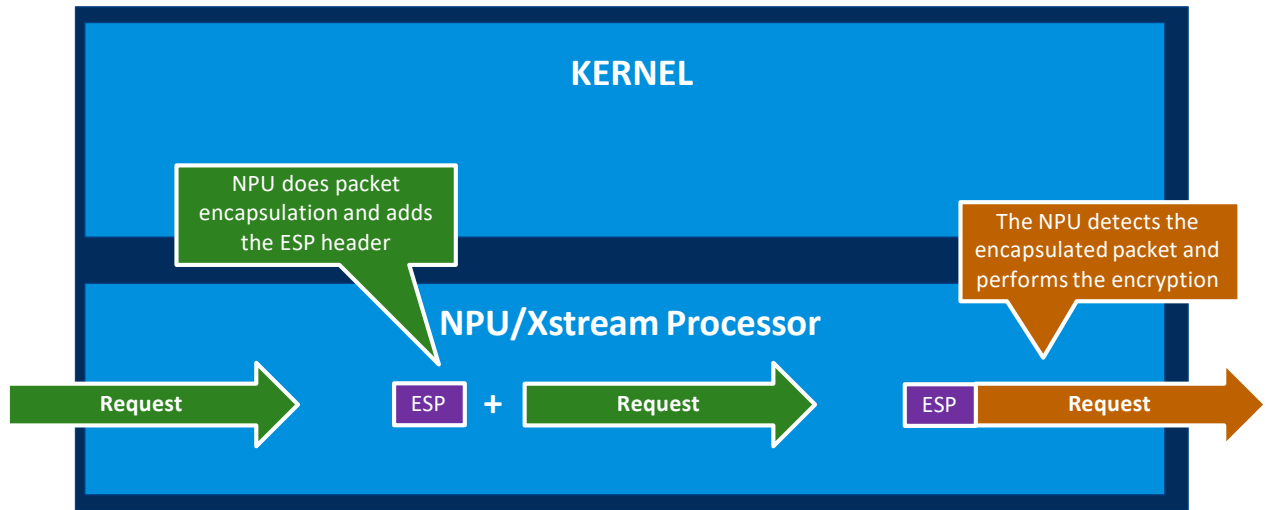
Com a aceleração IPsec habilitada, quando um pacote chega no kernel ainda executará o encapsulamento, mas não criptografará o pacote.

A NPU detectará o cabeçalho ESP e executará a criptografia no pacote.

O inverso acontecerá com a resposta. A NPU descriptografará o pacote e o kernel removerá o encapsulamento.

# IPsec Acceleration with Firewall Acceleration (FastPath)

## SOPHOS FIREWALL



SOPHOS

Se você também tiver a aceleração de firewall habilitada, descarregando para o FastPath, a NPU fará o encapsulamento de pacotes e criptografia. Este é o cenário ideal.

O oposto é verdadeiro com a aceleração IPsec e a aceleração de firewall desativadas, pois o kernel fará o encapsulamento e a criptografia.