



Getting Started with Firewall and NAT Rules on Sophos Firewall

Sophos Firewall
Version: 19.0v2

Firewall Rules



As regras de firewall e NAT são processadas em ordem



A primeira regra a corresponder é usada



Se não houver uma regra de firewall correspondente, o tráfego será descartado

SOPHOS

Para permitir o tráfego de rede dentro e fora da rede através de um firewall, você geralmente precisa de duas coisas; uma regra de firewall e uma regra NAT.

Quando você começa a configurar regras de firewall e NAT no Sophos Firewall, há três coisas importantes a serem lembradas:

As regras são processadas em ordem de cima para baixo

A primeira regra a corresponder é usada

E se não houver nenhuma regra de firewall correspondente, o tráfego será descartado

A regra de descarte padrão não pode ser editada e não registra o tráfego. Se você quiser registrar o tráfego descartado, precisará criar uma regra de firewall de descarte que corresponda a todo o tráfego e habilite o registro. Essa regra deve estar na parte inferior do conjunto de regras.

Para regras NAT, se não houver nenhuma regra de correspondência, nenhum NATing será aplicado ao tráfego. Ao contrário das regras de firewall, o tráfego não é bloqueado quando nenhuma regra NAT é correspondida.

Creating Firewall Rules

The screenshot shows the Sophos Firewall web interface. The left sidebar has a 'PROTECT' section with 'Rules and policies' highlighted. The main area is titled 'Rules and policies' and shows a list of firewall rules. The 'Add firewall rule' button is highlighted with an orange box, and a dropdown menu is open showing 'New firewall rule' and 'Server access assistant (DNAT)'. The table of rules includes columns for Rule type, #, Name, Source, Destination, and Action. The first two rules are DNAT rules for port 80 and port 8080. The third rule is an Automatic VPN Rule. The fourth rule is Traffic to Internal Network. The fifth rule is Traffic to WAN. The sixth rule is Traffic to DMZ.

Rule type	#	Name	Source	Destination	Action
DNAT	1	DNAT to 10.16.16.2...	WAN, Any host	LAN, #PortB	RDP33892
DNAT	2	DNAT to 10.16.16.1...	WAN, Any host	LAN, #PortB	RDP
Automatic VPN Rule	3	Automatic VPN Rule...	in 0 B, out 29.65 MB		
Traffic to Internal Network	1	Traffic to Internal Network	To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...		
Traffic to WAN	1	Traffic to WAN	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the default...		
Traffic to DMZ	1	Traffic to DMZ	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the default...		

Vamos começar analisando como criar uma regra básica de firewall. Neste exemplo, criaremos uma regra que permite o tráfego da Web de computadores na rede para a Internet.

Para começar, navegue até **PROTECT > Rules and policies**, then select **Add firewall rule**.

Creating Firewall Rules

Rule Properties

Matching Criteria

Exclusions

Linked NAT

Security Features

Feedback

How-to guides

Log viewer

Help

admin

Sophos

Add firewall rule

☒ Enable rule

Rule name *

Desktops to Internet

Action

Accept

☒ Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description

Allow web traffic from the desktop network to the Internet

Rule position

Bottom

Rule group

Automatic

Automatically adds rule to an existing group based on first match with rule type and source-destination zones.

☒ This rule will be added automatically to Traffic to WAN rule group.

SOPHOS

Na seção superior, você configura as propriedades, incluindo a posição da regra, o grupo, a ação e a se deseja registrar o tráfego da regra.

Por padrão, o Sophos Firewall tentará colocar a regra no grupo mais apropriado com base na configuração da zona de origem e destino e no tipo de regra de firewall.

Creating Firewall Rules

Rule Properties

Matching Criteria

Exclusions

Linked NAT

Security Features

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *

LAN

Add new item

Source networks and devices *

Endpoints-172-17-17

Add new item

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *

WAN

Add new item

Destination networks *

Any

Add new item

Services *

HTTP

HTTPS

Add new item

Services are traffic types based on a combination of protocols and ports.

☐ Match known users

SOPHOS

Os critérios de correspondência para a regra de firewall abrangem as zonas de origem e de destino e a rede, e a capacidade de agendar quando a regra estará ativa.

Você também pode corresponder em usuários e grupos. Por enquanto, vamos nos concentrar na configuração de uma regra de firewall de rede.

Creating Firewall Rules

Rule Properties

Matching Criteria

Exclusions

Linked NAT

Security Features

▼ Add exclusion

Source zones

Add new item

Source networks and devices

Add new item

Destination zones

Add new item

Destination networks

Add new item

Services

Add new item

Services are traffic types based on a combination of protocols and ports.

SOPHOS

Você pode excluir zonas, redes e serviços específicos de serem correspondidos pela regra de firewall. Isso simplifica a criação de regras de firewall onde há exceções, pois você pode criar uma única regra genérica e adicionar exclusões, enquanto seriam necessárias várias regras se as exclusões não estivessem disponíveis.

Creating Firewall Rules

Rule Properties

Matching Criteria

Exclusions

Linked NAT

Security Features

The screenshot shows the 'Create linked NAT rule' configuration page in the Sophos Firewall interface. The page has a grey header with the title 'Create linked NAT rule' and a help icon. Below the header is a white form area. At the top of the form is a blue button labeled 'Add NAT rule'. Below this is a section with a toggle switch for 'Enable rule' (currently on) and three input fields: 'Rule name *' (with a placeholder 'Enter Rule name'), 'Description', and 'Rule position' (a dropdown menu set to 'Top'). Below these fields is a horizontal line. Under the line is the section 'Translation settings' with a sub-header 'Select the matching criteria and translation settings for source, destination, and services.' Below this is a blue information icon followed by a text box stating: 'All the matching criteria of firewall, including users and schedule apply to its linked NAT rule. Can't edit these in the NAT rule.' Below this text box are four input fields arranged in a 2x2 grid. The top-left field is 'Original source *' with a dropdown menu set to 'Any' and an 'Add new item' link below it. The top-right field is 'Translated source' with a dropdown menu set to 'MASQ'. The bottom-left field is 'Original destination *' with a dropdown menu set to 'Any' and an 'Add new item' link below it. The bottom-right field is 'Translated destination' with a dropdown menu set to 'Original'.

SOPHOS

Você pode criar regras NAT vinculadas a regras de firewall. Aqui você só precisa configurar o NAT de origem, pois todas as fontes, destinos e serviços terão os mesmos critérios de correspondência que a regra de firewall.

As regras NAT vinculadas são projetadas principalmente para garantir uma migração suave de versões anteriores do Sophos Firewall, onde a configuração NAT foi concluída como parte da regra de firewall. Para obter o benefício total do Sophos Firewall, recomendamos não criar novas regras NAT vinculadas. Abordaremos a criação de regras NAT em breve.

Creating Firewall Rules

Rule Properties

Matching Criteria

Exclusions

Linked NAT

Security Features

Security features

› Web filtering

› Configure Synchronized Security Heartbeat

Other security features

Identify and control applications (App control)

None

☐ Apply application-based traffic shaping policy

Shape traffic

None

DSCP marking

Select DSCP marking

Detect and prevent exploits (IPS)

None

› Scan email content

SOPHOS

No final da regra de firewall, você pode habilitar recursos de segurança e selecionar políticas para filtragem da Web, Security Heartbeat, IPS, controle de aplicativos e muito mais.

Simulação: Criar uma regra de firewall



Nesta simulação, você criará regras de firewall da maneira mais protegida possível, uma para saída do seu MAC, depois criará regras por grupo pré-definidas conforme quadro inicial.

LAUNCH SIMULATION

CONTINUE

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

SOPHOS

Nesta simulação, você modificará a regra de firewall padrão para permitir o tráfego de saída de zonas adicionais e, em seguida, criará regras de firewall para permitir o tráfego de e para a filial de Nova York pelo MPLS.

Managing Firewall Rules

Rule type		Source zone	Destination zone	Status	Rule ID	Add Filter		Reset filter
#	Name	Source	Destination	What	ID	Action	Feature and service	
	Traffic to Interna... in 0 B, out 0 B	Traffic to LAN and WiFi Zones						
1	Drop from DMZ to L... in 0 B, out 0 B	DMZ, Any host	LAN, Any host	Any service	#4	Reject	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	
2	Website from Inter... in 0 B, out 0 B	Any zone, Any host	#eth1	www.sophotraining.x	#9	Forward	[IPS] [AV] [WEB] [APP] [DOS] [NAT] [LOG] [IPS]	
3	Allow all from lap... in 744.34 MB, out 101...	LAN, Laptop	Any zone, Any host	Any service	#7	Accept	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	
	Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...						
4	{example}-Traffic... in 0 B, out 0 B	Any zone, Any host	WAN, Any host	Any service	#3	Drop	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	
5	Endpoints to Inter... in 0 B, out 0 B	LAN, Endpoints-172-17-17, Any L...	WAN, Any host	HTTP, HTTPS	#8	Accept	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	
	Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...						
6	{example}-Traffic... in 0 B, out 0 B	Any zone, Any host, Any live user...	DMZ, Any host	Any service	#2	Drop	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	
7	Auto added firewal... in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	[AV] [WEB] [APP] [DOS] [H1] [NAT] [LOG] [IPS]	

SOPHOS

Agora que você viu como criar uma regra de firewall, vamos dar uma olhada em como você pode gerenciar as regras de firewall.

Você pode ver os principais detalhes, como origem, destino e serviço para cada uma das regras de firewall, e onde um campo é truncado, você pode passar o mouse sobre ele para ver o conteúdo completo.

A direita, você pode ver quais recursos foram habilitados dentro da regra de firewall e, se passar o mouse sobre isso, poderá ver um resumo completo da regra.

Managing Firewall Rules

Rule position	Name	Source	Destination	What	ID	Action	Feature and service
#	Traffic to Interna... in 0 B, out 0 B		Traffic to LAN and WiFi Zones				
1	Drop from DMZ to L...				#4	Reject	AV, WEB, APP, QOS, NAT, LOG, IPS
2	Website from Inter...			straining.x)	#9	Forward	IPS, AV, WEB, APP, QOS, NAT, LOG
3	Allow all from lap...				#7	Accept	AV, WEB, APP, QOS, NAT, LOG, IPS
4	example-Traffic...				#3	Drop	AV, WEB, APP, QOS, NAT, LOG, IPS
5	Endpoints to Inter...				#8	Accept	AV, WEB, APP, QOS, NAT, LOG, IPS
6	example-Traffic...	Any zone, Any host, Any live user...	DMZ, Any host	Any service	#2	Drop	AV, WEB, APP, QOS, NAT, LOG, IPS
7	Auto added firewal...			(S)	#1	Accept	AV, WEB, APP, QOS, NAT, LOG, IPS

SOPHOS

Há dois números para cada regra de firewall, o primeiro é a posição da regra, e isso será atualizado se você mover uma regra, o que pode ser feito arrastando-as e soltando-as. A segunda é a ID da regra, esta é a referência exclusiva das regras e não será alterada. O importante a notar é que o ID da regra não reflete a posição da regra; eles podem ser, e geralmente serão, diferentes.

Você notará que as regras de firewall usam ícones diferentes, ícones verdes para regras de permissão, vermelho para soltar ou rejeitar e cinza para desabilitado.

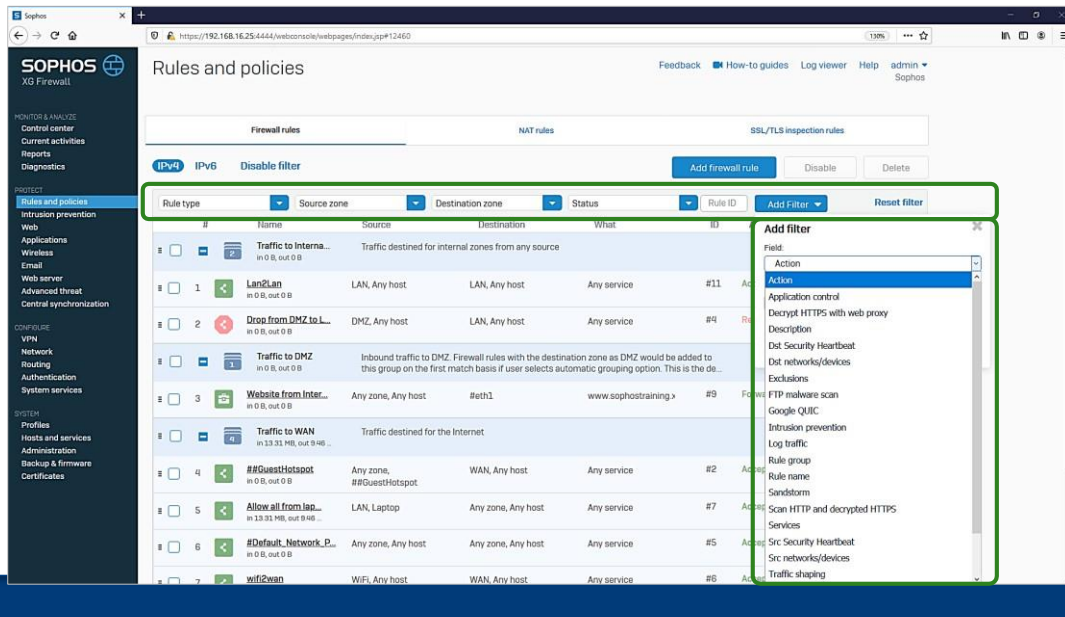
Cada ícone também mostra que tipo de regra é:

Regra de firewall de proteção de servidor Web, para proteger servidores Web

Regra de rede, em que o tráfego é correspondido apenas em propriedades de rede

Regra de usuário, em que o Sophos Firewall também corresponde à identidade do usuário

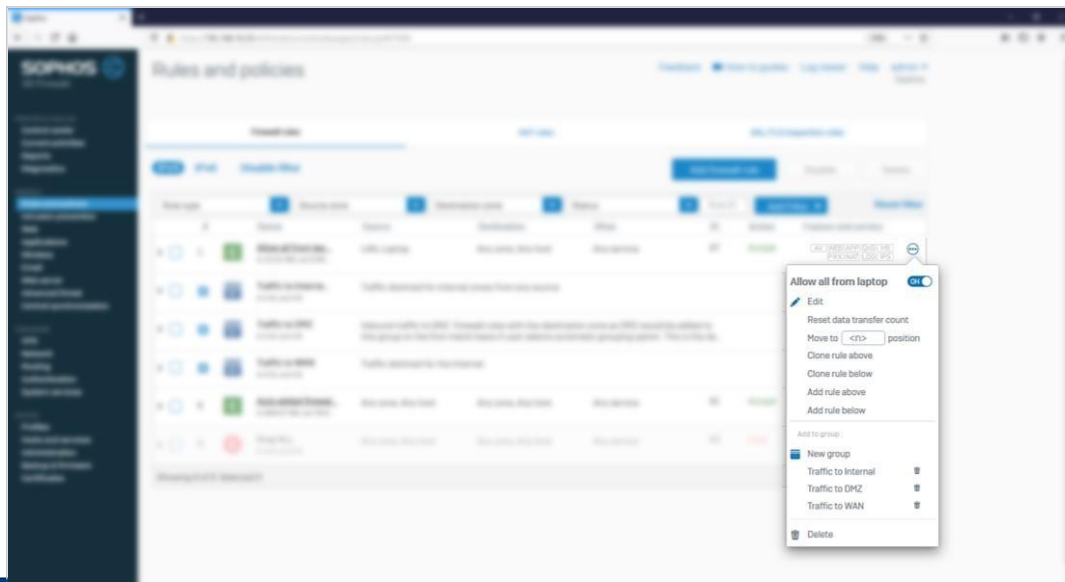
Managing Firewall Rules



Na parte superior da guia Regras de firewall estão filtros comuns que podem ser aplicados usando a lista suspensa

Menus. Você também pode adicionar filtros mais detalhados com base em qualquer campo na regra de firewall.

Managing Firewall Rules

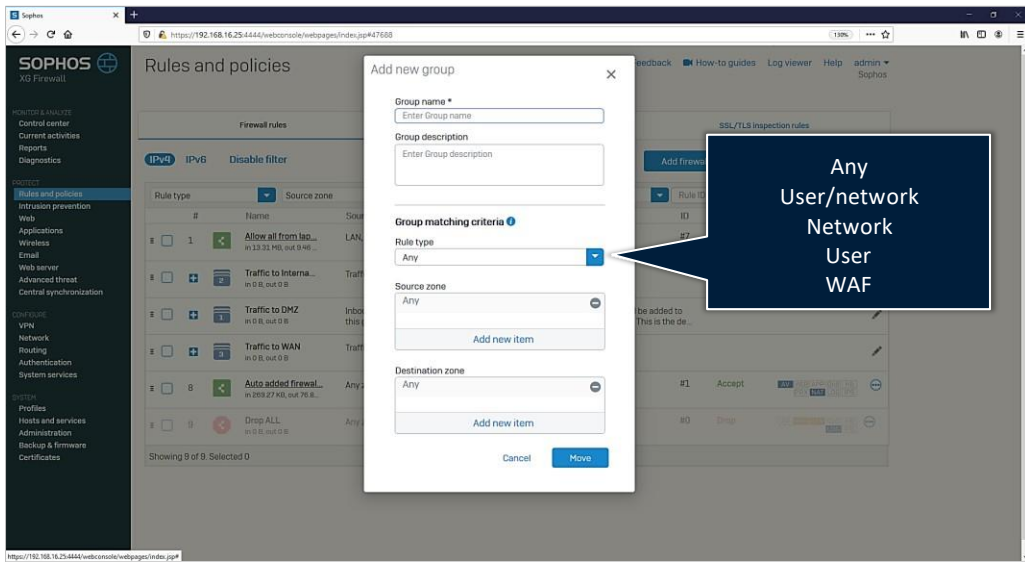


SOPHOS

No lado direito de cada regra há um menu de elipses que fornece controles adicionais, incluindo:

- * Redefinir o contador de dados da regra, o que pode ser útil ao solucionar problemas
- * Movendo a regra para uma posição específica
- * Clonando a regra
- * Adicionando uma nova regra acima ou abaixo dela
- * Adicionar a regra a um grupo ou desanexá-la de um grupo
- * E excluir, habilitar ou desabilitar a regra

Managing Firewall Rules



SOPHOS

Quando analisamos a criação de uma regra de firewall, dissemos que o Sophos Firewall tentará adicionar a regra ao grupo mais apropriado com base na configuração selecionada.

Para adicionar um novo grupo, use a opção no menu de reticências. Aqui você pode configurar os critérios de correspondência que serão usados para atribuir regras a grupos automaticamente.

NAT Rules

Você pode criar uma regra NAT vinculada que corresponda aos mesmos critérios que a regra de firewall à qual ela está vinculada

Recomendamos configurar regras NAT de forma independente usando a tabela NAT

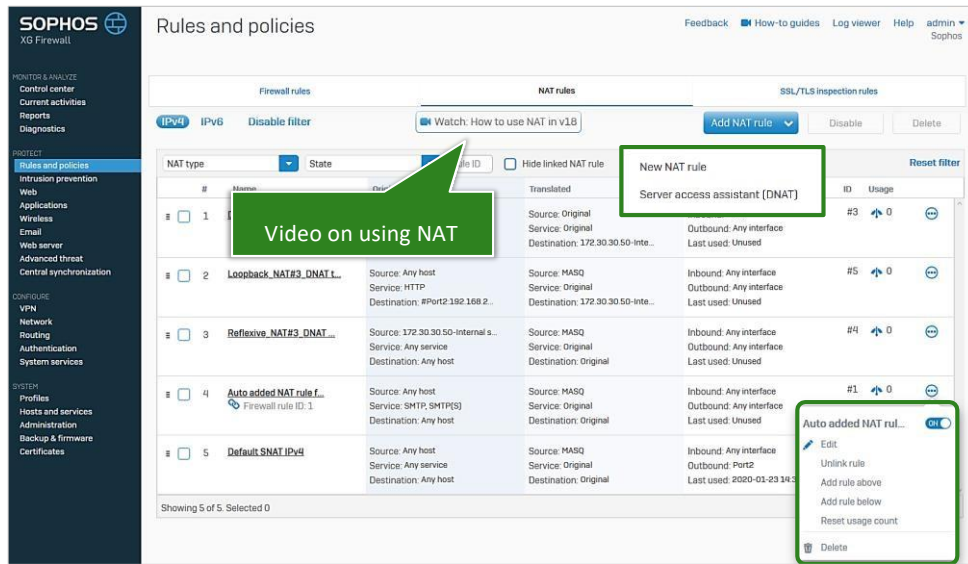
As regras NAT ainda exigem regras de firewall para permitir o tráfego

SOPHOS

Você pode criar regras NAT vinculadas para NATing de origem de dentro da configuração da regra de firewall; no entanto, isso é projetado principalmente para oferecer suporte à migração de configuração da versão 17.5. Recomendamos configurar regras NAT independentemente usando a tabela NAT para oferecer suporte a cenários de configuração mais poderosos e flexíveis, incluindo SNAT (NAT de origem) e DNAT (NAT de destino) em uma única regra. As regras NAT ainda exigem uma regra de firewall para permitir o tráfego!

Você geralmente precisa de muito menos regras NAT do que regras de firewall, portanto, criá-las separadamente permite simplificar sua configuração. Em ambientes simples, você pode precisar apenas de uma única regra geral de saída mascarada, em vez de configurá-la individualmente em cada regra de firewall.

Managing NAT Rules



SOPHOS

Na guia NAT, você pode gerenciar o conjunto de regras NAT, reordenar as regras e ver quantas conexões

cada uma das regras foi traduzida.

No menu de cada regra, você pode redefinir o contador de uso e, no caso de regras NAT vinculadas, desvinculá-las da regra de firewall associada.

Ao adicionar regras NAT, você pode criar uma regra NAT ou, para cenários DNAT, usar o assistente de acesso ao servidor para criar a regra de firewall e as regras NAT.

Há também um botão na parte superior da página para um vídeo que explica a configuração do NAT em profundidade.

Configuring NAT Rules

Translation settings

Select the matching criteria and translation settings for source, destination, and services.

Original source *	Original destination *	Original service *
Any	Any	Any
Add new item	Add new item	Add new item

Translated source (SNAT)	Translated destination (DNAT)	Translated service (PAT)
Original	Original	Original

Interface matching criteria

Inbound interface *	Outbound interface *
Any	Any
Add new item	Add new item

☒ Override source translation (SNAT) for specific outbound interfaces

Outbound interface	Translated source
XG2Lan	Branch Office

☐ Create loopback rule

☐ Create reflexive rule

Matching criteria

Translations

Matching criteria

Override source translation for specific outbound interfaces

SOPHOS

Dentro da regra NAT, você configura os critérios de correspondência na origem, destino e serviço originais e quaisquer traduções que precisem ser feitas. Esse design permite que você configure o NATing de origem, destino, serviço e interface em uma única regra.

Você também pode fazer a correspondência nas interfaces de entrada e saída.

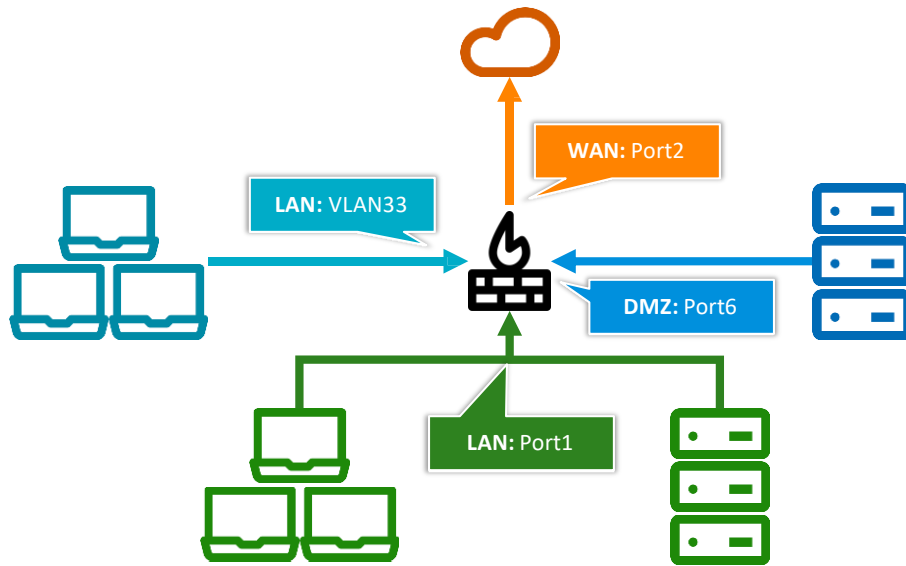
Ao habilitar a opção Substituir conversão de origem para interfaces de saída específicas, você pode selecionar NATs de origem diferentes com base na interface de saída, tudo dentro de uma única regra.

Na parte inferior da regra NAT, você pode, opcionalmente, optar por criar um: Política de loopback: quando o usuário interno deseja acessar um servidor interno usando seu nome de host público ou endereço IP

Política reflexiva: permite que o tráfego atravesse o NAT na direção oposta

Na seção Avançado estão as configurações de balanceamento de carga para a regra NAT. Isso só pode ser configurado quando o destino é um intervalo de IP.

Masquerading SNAT Scenario



SOPHOS

Vamos considerar um cenário de exemplo em que queremos executar um SNAT mascarado em todos os tráfegos saindo na porta WAN2. Podemos criar uma única regra NAT para isso.

Default SNAT Rule

Rule status

Rule name *

Default SNAT (IPv4)

Description

Auto created IPv4 SNAT MASQ rule for traffic from "ANY" inbound interface to WAN outbound interface. If both inbound and outbound are WAN, it will be MASQ.

Translation settings

Select the matching criteria and translation settings for source, destination, and services.

Original source *

Any

Add new item

Original destination *

Any

Add new item

Original service *

Any

Add new item

Translated source (SNAT)

MASQ

Translated destination (DNAT)

Original

Translated service (PAT)

Original

Interface matching criteria

Inbound interface *

Any

Add new item

Outbound interface *

Port2

Add new item

☐ Override source translation (SNAT) for specific outbound interfaces ⓘ

Translation

Matching criteria

SOPHOS

Aqui você pode ver a regra SNAT padrão que satisfaz o cenário. A regra corresponde ao interface de saída e aplica a política MASQ NAT ao endereço de origem. MASQ é a política de mascaramento padrão e alterará o endereço IP de origem para ser o mesmo que a interface pela qual o tráfego está deixando.

Simulação: Configurar regras NAT

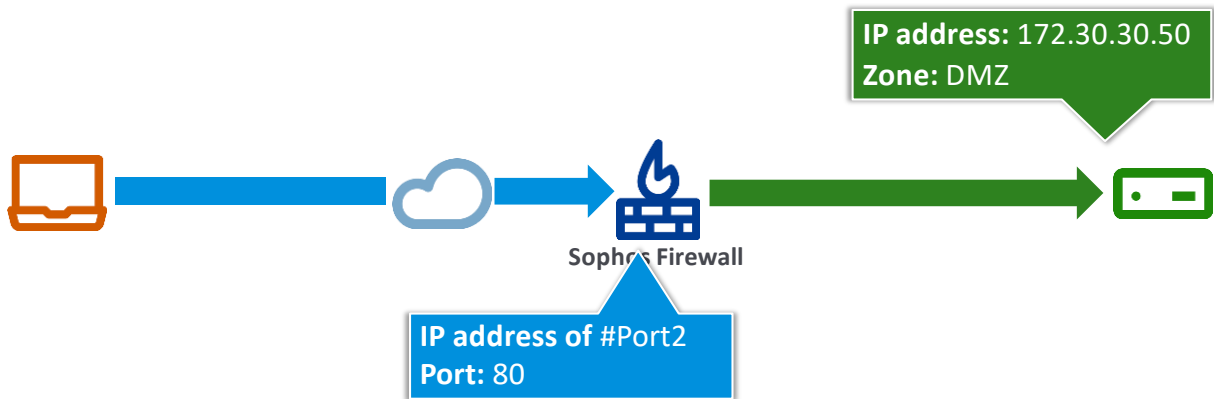


Nesta simulação, removerá uma regra padrão de NAT e criará uma regra NAT para o tráfego manualmente.

SOPHOS

Nesta simulação, você removerá a regra NAT vinculada para a regra de firewall padrão, desvinculará o NAT para proteção de email e crie uma regra NAT para o tráfego MPLS.

DNAT Scenario



SOPHOS

Outro caso de uso comum é usar NAT de destino, ou DNAT, para publicar um aplicativo na Internet. Para fazer isso, você usará uma regra de firewall de rede para permitir que o tráfego e uma regra NAT executem a conversão de destino.

Se olharmos para um exemplo, podemos ter um aplicativo baseado na Web em um servidor interno na DMZ que desejamos publicar em um endereço IP público atribuído na porta WAN, isso é #Port2.

Quando o usuário se conecta à porta 80 usando o endereço IP público, queremos alterar o destino para o servidor interno e enviar o tráfego ligado.

Server Access Assistant (DNAT)

Internal Server IP address

Specify the private IP address of the internal server to access from the internet.


☐ Select IP host

☒ 172.30.30.50 [Creates an IP host with the specified IP address and name.]

IP host name

IP address: 172.30.30.50

Zone: DMZ




Server

Public IP address

Specify the public IP address through which users can access the server.

☒ #Port2 - 192.168.254.200

☐ Type IP [Creates an IP host with the specified IP address and name.]



XG Firewall

IP address of #Port2
Port: 80

SOPHOS

Vamos dar uma olhada no uso do assistente de acesso ao servidor para criar um DNAT e uma regra de firewall para isso cenário.

Comece selecionando o servidor interno ou insira o endereço IP e um objeto de host IP será criado para ele.

Escolha a interface à qual os usuários se conectarão ao acessar o servidor interno. Como alternativa, você pode inserir o endereço IP ao qual os usuários se conectarão e um objeto de host IP será criado para ele.

Server Access Assistant (DNAT)

Services

Users can access the selected services on the internal server.

HTTP

Add new item

External source networks and devices

Users can access the internal server from the selected source networks and devices.

Any

Add new item

SOPHOS

Selecione os serviços que você deseja acessar no servidor interno e as redes de origem permitidas.

Server Access Assistant (DNAT)

Review your selection

Select Save to add NAT rules and firewall rules with the following configuration:

Internal server to access from the internet:

IP host: **172.30.30.50**

Hostname: **172.30.30.50-Internal server**

Public IP address through which users access the internal server:

IP host: **192.168.254.200**

Hostname: **#Port2**

Services that users can access:

HTTP

Sources from which users can access the server:

Any

Creates three NAT rules:

Inbound NAT (DNAT): Traffic destined to the public IP address **192.168.254.200** is translated to the internal server address **172.30.30.50**

Outbound NAT (SNAT): Masquerades outbound traffic from the internal server **172.30.30.50** with the public IP address **192.168.254.200**

Loopback NAT: Internal network uses the same public IP address **192.168.254.200** to access the internal server **172.30.30.50**

Creates one firewall rule:

Allows access to the internal server for **HTTP** services from the sources **Any**.

The rules are added at the top of the table and are turned on by default.

SOPHOS

Revise o resumo da configuração selecionada e clique em Salvar e concluir.

DNAT Firewall Rule

The screenshot shows the configuration page for a DNAT Firewall Rule in the Sophos Firewall management console. The interface is divided into several sections:

- Rule status:** Includes a toggle for 'Rule status' (currently ON), a 'Rule name' field with the value 'DNAT to 172.30.30.50-internal server_3578789827', a 'Description' field with the value 'DNAT rule created using DNAT wizard. DNAT to 172.30.30.50-internal server', and a 'Rule group' dropdown set to 'None'.
- Action:** Includes an 'Action' dropdown set to 'Accept' and a checkbox for 'Log firewall traffic' (currently unchecked).
- Source:** Includes a 'Source zones' field with 'WAN' selected, a 'Source networks and devices' field with 'Any' selected, and a 'During scheduled time' dropdown set to 'All the time'.
- Destination and services:** Includes a 'Destination zones' field with 'DMZ' selected, a 'Destination networks' field with '#Port2' selected, and a 'Services' field with 'HTTP' selected.

Two green callout boxes highlight specific configuration details:

- A callout box labeled 'Zone of internal server' points to the 'DMZ' selection in the 'Destination zones' field.
- A callout box labeled 'Interface on the Sophos Firewall' points to the '#Port2' selection in the 'Destination networks' field.

SOPHOS

Aqui você pode ver a regra de firewall criada pelo assistente de acesso ao servidor.

Observe que a zona de destino é a zona em que o servidor interno está, essa é a zona após a NATing ter ocorrido. A rede de destino é a interface no Sophos Firewall à qual o usuário se conectará, este é o endereço IP antes que o NATing tenha ocorrido.

Você pode editar essa regra de firewall e habilitar proteção adicional, como IPS.

DNAT Rules

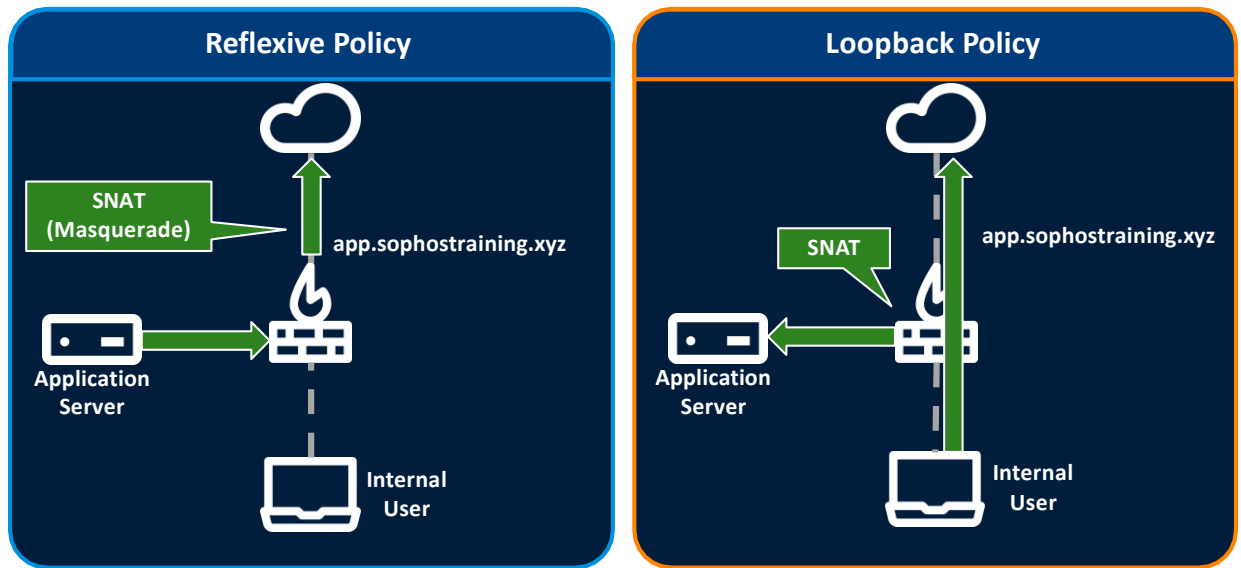
NAT type		State	Rule ID	<input type="checkbox"/> Hide linked NAT rule		Reset filter	
#	Name	Original	Translated	Interface	ID	Usage	
<input type="checkbox"/> 1	DNAT to 172.30.30.50-...	Source: Any host Service: HTTP Destination: #Port2:192.168.2...	Source: Original Service: Original Destination: 172.30.30.50-Inte...	Inbound: Port2 Outbound: Any interface Last used: Unused	#3	0	
<input type="checkbox"/> 2	Loopback_NAT#3_DNAT t...	Source: Any host Service: HTTP Destination: #Port2:192.168.2...	Source: MASQ Service: Original Destination: 172.30.30.50-Inte...	Inbound: Any interface Outbound: Any interface Last used: Unused	#5	0	
<input type="checkbox"/> 3	Reflexive_NAT#3_DNAT ...	Source: 172.30.30.50-Internal s...	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#4	0	

SOPHOS

Aqui você pode ver as três regras NAT criadas pelo assistente de acesso ao servidor, a regra DNAT, a regra de loopback e a regra reflexiva.

Você pode modificar ainda mais a regra DNAT. Por exemplo, você também pode querer traduzir a porta.

Reflexive and Loopback Policies



SOPHOS

Regras reflexivas criam um SNAT a partir de fontes internas, por exemplo, de um servidor protegido para a Internet. Em nosso exemplo anterior, ele efetivamente criaria uma regra mascarada para o tráfego do servidor de aplicativos.

As regras de loopback são usadas quando os usuários internos usam o endereço IP público ou o nome do host para acessar um recurso e ele executa um SNAT na conexão.

Elas só podem ser criadas automaticamente ao criar novas regras NAT e não ao editar.

Simulação: Criar uma regra DNAT usando o Acesso ao Servidor - Assistente



Nesta simulação, você publicará um servidor usando uma regra DNAT criada usando o assistente de acesso ao roteador wireless na porta 80.

LAUNCH SIMULATION

CONTINUE

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

SOPHOS

Nesta simulação, você publicará um servidor usando uma regra DNAT criada usando o acesso ao servidor assistente.