



Getting Started with Intrusion Prevention on Sophos Firewall

Sophos Firewall

Version: 19.0v1

Intrusion Prevention Overview



Políticas do sistema de prevenção de intrusões (IPS)



Proteção contra falsificação



Proteção contra negação de serviço (DoS)

SOPHOS

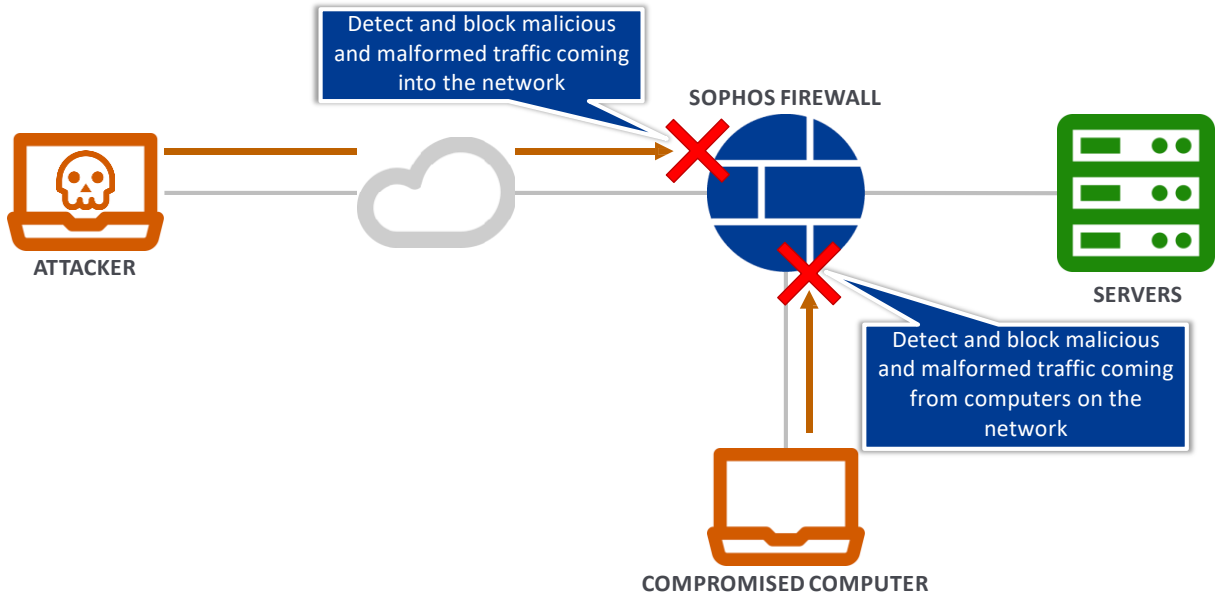
A prevenção de intrusões no Sophos Firewall tem três partes:

Políticas do sistema de prevenção de intrusões, ou IPS, que são aplicadas às regras de firewall para proteger contra explorações e tráfego malformado

Proteção contra falsificação, que descarta o tráfego que está tentando fingir vir de um endereço MAC ou IP diferente para ignorar a proteção

E a proteção DoS de negação de serviço, que derruba o tráfego que está maliciosamente tentando impedir que o tráfego legítimo possa acessar os serviços

IPS Policies



SOPHOS

Vamos começar com as políticas de IPS.

As políticas IPS são uma coleção de regras para detectar dados mal-intencionados e malformados que podem explorar computadores e servidores. As diretivas IPS são selecionadas nas regras de firewall, para que possam ser usadas para proteger contra ataques ao tráfego que entra na rede e tráfego proveniente de computadores comprometidos na rede.

Enabling IPS

The screenshot displays the Sophos Firewall web interface. The left sidebar shows the 'Intrusion prevention' menu item highlighted. The main content area is titled 'Intrusion prevention' and contains a tabbed interface with 'IPS policies' selected. The 'IPS protection' toggle is shown in two states: 'OFF' and 'ON'. A blue arrow points from the 'OFF' state to the 'ON' state. The 'ON' state shows 'Firewall rules using IPS' as '1' and 'Time of signature update' as '10:04:00, Jan 31 2022'.

SOPHOS

Antes de configurar e usar a prevenção contra invasões, você precisa habilitar a proteção IPS. Isso fará o download das assinaturas IPS para o Sophos Firewall. Uma vez que as assinaturas tenham sido baixadas, elas serão mantidas atualizadas.

Se o IPS estiver desativado por meio do switch, as assinaturas IPS serão removidas após 30 dias, a menos que sejam habilitadas novamente.

Out-of-the-Box IPS Policies

IPS policies are configured in:
PROTECT > Intrusion prevention > IPS policies

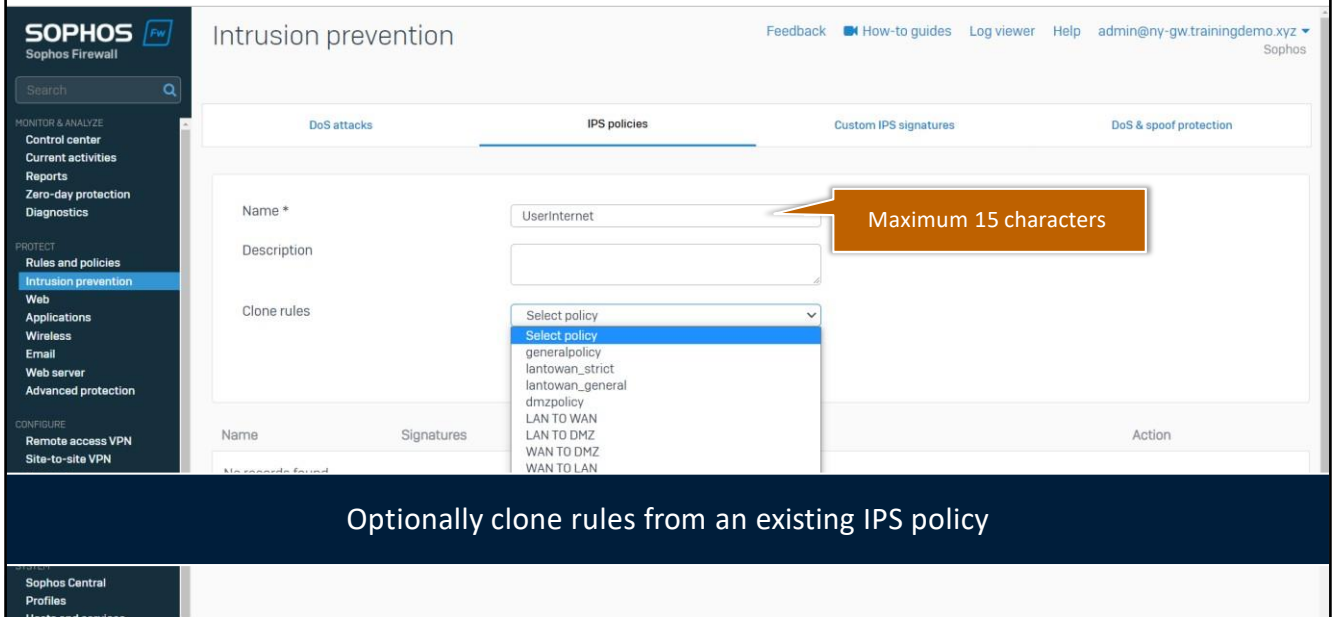
The screenshot displays the Sophos Firewall web interface. The main heading is 'Intrusion prevention'. Below it, there are four tabs: 'DoS attacks', 'IPS policies' (which is selected), 'Custom IPS signatures', and 'DoS & spoof protection'. The 'IPS policies' tab shows a table of predefined policies. Each row includes a checkbox, a 'Name' column, a 'Description' column, and a 'Manage' column with edit and delete icons. The policies listed are: DMZ TO LAN, DMZ TO WAN, LAN TO DMZ, LAN TO WAN, WAN TO DMZ, WAN TO LAN, and dmzpolicy. The left sidebar contains a navigation menu with sections like 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'PROTECT' section has 'Rules and policies' expanded, with 'Intrusion prevention' selected. The top right corner shows a user profile for 'admin@ny-gw.trainingdemo.xyz'.

<input type="checkbox"/>	Name	Description	Manage
<input type="checkbox"/>	DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN; Primarily intended to secure server(s) hosted in the LAN zone	
<input type="checkbox"/>	DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN; Primarily intended to secure the DMZ-based client(s)	
<input type="checkbox"/>	LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ; Primarily intended to secure the LAN-based client(s) and DMZ-based server(s)	
<input type="checkbox"/>	LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN; Primarily intended to secure LAN-based client(s)	
<input type="checkbox"/>	WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ; Primarily intended to secure server(s) hosted in the DMZ	
<input type="checkbox"/>	WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN; Primarily intended to secure server(s) hosted in the LAN	
<input type="checkbox"/>	dmzpolicy	A General policy to scan traffic flowing to DMZ	

O Sophos Firewall vem com várias políticas IPS predefinidas, que podem ser encontradas em **PROTECT > Intrusion prevention > IPS policies**.

Essas políticas cobrem a maioria dos cenários cotidianos que você encontraria em uma rede média. Você pode editar as políticas incluídas ou criar novas para atender às suas necessidades de segurança.

Creating IPS Policies



The screenshot displays the Sophos Firewall web interface for configuring Intrusion Prevention (IPS) policies. The left sidebar shows the navigation menu with 'Intrusion prevention' selected. The main content area is titled 'Intrusion prevention' and has tabs for 'DoS attacks', 'IPS policies', 'Custom IPS signatures', and 'DoS & spoof protection'. The 'IPS policies' tab is active, showing a form to create a new policy. The 'Name' field is highlighted with a callout box indicating a maximum of 15 characters. The 'Description' field is empty. The 'Clone rules' dropdown menu is open, showing a list of existing policies to clone from. Below the form, there is a table with columns for 'Name', 'Signatures', and 'Action'. A dark blue banner at the bottom of the interface states: 'Optionally clone rules from an existing IPS policy'.

Ao criar uma nova política de IPS, você dá a ela um nome, limitado a quinze caracteres, e uma descrição. Em seguida, você pode, opcionalmente, selecionar para clonar as regras de uma política existente. Isso pode economizar muito tempo ao criar novas políticas. Você precisa salvar a política neste ponto para que, se você tiver selecionado clonar regras, elas possam ser adicionadas. Em seguida, você pode editar a política.

Configuring IPS Policies

SOPHOS Sophos Firewall

Intrusion prevention

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz Sophos

DoS attacks **IPS policies** Custom IPS signatures DoS & spoof protection

Name * UserInternet

Description

Save Cancel

Drag and drop to order rules

<input type="checkbox"/>	Name	Signatures	Signature filter criteria	Action	Manage
<input type="checkbox"/>	Browsers_Officetools_Multi... and Instant Messaging	All	Category = browser-ie, browser-... Severity = All Severity Platform = All Platform Target = Client	Recommended	
<input type="checkbox"/>	Operating System and Services	All	Category = os-windows, indicato... Severity = All Severity Platform = All Platform	Recommended	

A política é composta por uma lista ordenada de regras. Cada regra contém uma ou mais assinaturas e tem uma ação. Você pode alterar a ordem das regras dentro da política arrastando-as e soltando-as.

Creating IPS Policy Rules

SOPHOS Firewall

Intrusion prevention

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz

DoS attacks **IPS policies** Custom IPS signatures DoS & spoof protection

Add IPS policy rules

Rule name * Windows Browsers

Category Severity Platform Target Smart filter Clear filter

Category: browser-chrome browser-firefox browser-ie browser-other browser-plugins browser-webkit Severity: Critical Major Moderate Minor Platform: Windows Target: Client

☒ Select all ☐ Select individual signatures

All filtered signatures or selected signatures only

Free-text filter

Name	SID	Category	Severity	Platform	Target	Recommended action
<input checked="" type="checkbox"/> BROWSER-CHROME Chrome CVE-2021-30551 Type Confusion in V8	2305826	browser-chrome	1 - Critical	Windows	Client	Drop packet
<input checked="" type="checkbox"/> BROWSER-CHROME Chrome Object Lifecycle Issue CVE-2021-21166 In Audio	2305825	browser-chrome	1 - Critical	Windows	Client	Drop packet

Ao adicionar ou editar uma regra, você pode selecionar rápida e facilmente os padrões IPS desejados por categoria, gravidade, plataforma e tipo de destino, com suporte para listas de filtros inteligentes persistentes que serão atualizadas automaticamente à medida que novos padrões forem adicionados que correspondam aos critérios selecionados.

Por exemplo, você pode usar o filtro inteligente para selecionar todas as assinaturas relacionadas a um aplicativo específico.

Você pode optar por incluir todas as assinaturas retornadas pelos filtros ou apenas assinaturas selecionadas. Observe que, se você escolher apenas assinaturas selecionadas, a regra não poderá atualizar as assinaturas incluídas automaticamente.

O Sophos Firewall inclui a biblioteca de assinaturas IPS comerciais Talos da Cisco. Aumentamos a biblioteca Talos com assinaturas adicionais, conforme necessário, para garantir a proteção ideal contra intrusões.

Talos é um grupo de análise de segurança de rede altamente respeitado que trabalha o tempo todo para responder às últimas tendências em hacking, invasões e malware... assim como o nosso próprio SophosLabs. Portanto, esta é uma ótima parceria que reforça nossa proteção IPS e fornece controles de política de IPS mais granulares.

Creating IPS Policy Rules

The screenshot displays the Sophos Firewall management console. On the left, a sidebar menu shows various sections: MONITOR & ANALYZE, PROTECT, CONFIGURE, and SYSTEM. The 'PROTECT' section is expanded, showing 'Rules and policies' and 'Intrusion prevention'. The main area shows the 'IPS policies' tab with a table of rules. The table has columns for 'DoS attacks', 'IPS policies', 'Custom IPS signatures', and 'DoS & spoof protection'. The 'IPS policies' column is active, showing a list of rules. A dropdown menu is open for the 'Action' column, showing options like 'Drop packet', 'Disable', 'Drop session', 'Reset', 'Bypass session', and 'Recommended'. The 'Recommended' option is highlighted. An orange callout box points to the 'Recommended' option with the text 'Recommended action for the signature'.

DoS attacks	IPS policies	Custom IPS signatures	DoS & spoof protection			
<input checked="" type="checkbox"/> BROWSER-CHROME Chrome CVE-2021-30551 Type Confusion in V8	2305826	browser-chrome	1 - Critical	Windows	Client	Drop packet
<input checked="" type="checkbox"/> BROWSER-CHROME Chrome Object Lifecycle Issue CVE-2021-21166 in Audio	2305825	browser-chrome	1 - Critical	Windows	Client	Drop packet
<input checked="" type="checkbox"/> BROWSER-CHROME Google Chrome Blink CVE-2020-6549 Renderer MediaElementEventLis... memory corruption attempt	2304641	browser-chrome	2 - Major	Windows	Client	Drop packet
<input checked="" type="checkbox"/> BROWSER-CHROME Google Chrome Blink CVE-2020-6549 MediaElementEventLis...	2304642	browser-chrome	2 - Major	Windows	Client	Drop packet

Recommended action for the signature

Na parte inferior da regra, você pode selecionar a ação que deseja executar. Uma dessas ações é 'Recomendado'. Você notará que cada assinatura tem uma ação recomendada associada a ela que pode ser usado ou você pode substituir isso com a ação aplicada à regra.

Applying IPS Policies

The screenshot shows the Sophos Firewall configuration interface. On the left is a dark sidebar with navigation menus: '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), and 'SYSTEM' (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware). The main area is titled 'Default Workplace Policy' and contains several sections. The 'Other security features' section includes dropdowns for 'Identify and control applications (App control)' (set to 'None'), 'Shape traffic' (set to 'User's policy applied'), and 'DSCP marking' (set to 'Select DSCP marking'). Below these is a checkbox for 'Apply application-based traffic shaping policy'. The 'Detect and prevent exploits (IPS)' dropdown is highlighted with an orange box, and a callout bubble points to it with the text 'Select an IPS policy for the firewall rule'. The dropdown currently shows 'UserInternet'. At the bottom are 'Save' and 'Cancel' buttons.

Depois de criar uma política IPS, ela precisa ser selecionada em uma regra de firewall para estar ativa. A regra de firewall selecionada determinará qual tráfego será verificado e a política de IPS determinará as verificações realizadas.

Simulação: Criar uma política de IPS



Nesta simulação, você criará uma política IPS e a aplicará a uma regra de firewall.

SOPHOS

Nesta simulação, você criará uma política de IPS e a aplicará a uma regra de firewall.

Spoof Protection

SOPHOS Firewall

Intrusion prevention

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz Sophos

DoS attacks IPS policies Custom IPS signatures DoS & spoof protection

Spoof protection general settings

☒ Enable spoof prevention

☒ Restrict unknown IP on trusted MAC

You need to add at least one MAC entry in the "Trusted MAC" list to enable MAC filtering

Drop packets that are not from a trusted MAC address

Drop if source IP does not match an entry on the firewalls routing table

	IP spoofing	MAC filter	IP-MAC pair filter
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ClientLAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If spoof protection is misconfigured, you can lock yourself out of the Sophos Firewall

Drop packets if source IP and MAC do not match trusted MAC address

Além da proteção que pode ser configurada nas políticas de IPS, há negação de serviço (DoS) e serviços de proteção contra falsificação que podem ser habilitados. Começaremos com a proteção de falsificação, que tem três modos de proteção que podem ser ativados por zona.

Falsificação de IP – os pacotes serão descartados se o endereço IP de origem não corresponder a uma entrada na tabela de roteamento de firewalls

Filtro MAC – os pacotes serão descartados se o endereço MAC de origem não estiver configurado como um MAC confiável

Filtro de par IP-MAC – os pacotes serão descartados se o IP e o MAC não corresponderem a nenhuma entrada em uma lista confiável IP-MAC

O filtro MAC não pode ser ativado até que pelo menos uma entrada seja adicionada à lista MAC confiável.

Além desses três modos, há a opção de restringir IP desconhecido no MAC confiável. Com essa opção ativada, qualquer tráfego de um endereço IP desconhecido em um endereço MAC confiável é descartado.

Por favor, note que, se a proteção contra falsificação estiver mal configurada, você pode se bloquear fora do Sophos Firewall!

Spoof Protection

SOPHOS Sophos Firewall

Intrusion prevention

Feedback How-to guides Log viewer Help admin@ny-gw.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

SYSTEM

- Sophos Central
- Profiles
- Hosts and services

DoS attacks IPS policies Custom IPS signatures **DoS & spoof protection**

Spoof protection trusted MAC

Add Delete Import

<input type="checkbox"/>	MAC address	IPv4 association	IPv4 address	IPv6 association	IPv6 address	Manage
<input type="checkbox"/>	00:0C:29:7D:03:EF	Static	172.16.16.10	None	-	

! If spoof protection is misconfigured, you can lock yourself out of the Sophos Firewall

Na seção MAC confiável de proteção contra falsificação, você pode adicionar endereços MAC que podem ser usados com o filtro MAC. Os endereços MAC podem ser associados a endereços IP; isso pode ser definido como nenhum, DHCP ou estático. Para endereços IP estáticos, você pode inserir vários valores.

Denial of Service (DoS) Protection

View dropped packet counters for each attack type

Attack type	Source			Source Traffic Dropped	Destination			Destination Traffic Dropped
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag		Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	
SYN flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
UDP flood	12000	100	<input type="checkbox"/>	0	18000	100	<input type="checkbox"/>	0
TCP flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
ICMP/ICMPv6 flood	120	100	<input type="checkbox"/>	0	300	100	<input type="checkbox"/>	0
Dropped source routed packets	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
Disable ICMP/ICMPv6 redirect packet	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
ARP hardening	-	-	-	-	-	-	<input type="checkbox"/>	-

Um ataque de negação de serviço (DoS) é um método que os hackers usam para impedir ou negar o acesso de usuários legítimos a um serviço. Os ataques DoS são normalmente executados enviando muitos pacotes de solicitação para um servidor de destino, o que inunda os recursos do servidor, tornando o sistema inutilizável. Seu objetivo não é roubar as informações, mas desativar ou privar um dispositivo ou rede para que os usuários não tenham mais acesso aos serviços/recursos da rede.

Todos os servidores podem lidar com o volume de tráfego até um máximo, além do qual eles se tornam desativados. Os invasores enviam um volume muito alto de tráfego redundante para um sistema para que ele não possa acompanhar o tráfego ruim e permitir o tráfego de rede permitido. A melhor maneira de se proteger contra um ataque DoS é identificar e bloquear esse tráfego redundante.

Aqui podemos ver a configuração para um ataque de inundação SYN. Você pode definir a taxa de pacotes permitida por minuto para cada origem e destino, bem como uma taxa de intermitência para cada origem e destino em pacotes por segundo.

Quando a taxa de intermitência é cruzada, o Sophos Firewall a considera como um ataque e fornece proteção contra ataques DoS, descartando todos os pacotes em excesso da origem ou do destino. O firewall continuará a descartar os pacotes até que o ataque diminua. Como o dispositivo aplica valores de limite por endereço IP, somente o tráfego da origem ou do destino será descartado. O restante do tráfego de rede continuará a ser processado normalmente.

Você pode exibir os contadores de pacotes descartados na guia Ataques DoS. Observe que a proteção DoS é aplicada globalmente a todo o tráfego que passa pelo Firewall Sophos.