



# Enabling Advanced Threat Protection on Sophos Firewall

**Sophos Firewall**

Version: 19.0v1

## Advanced Threat Protection (ATP) Overview



Detecte dispositivos comprometidos em sua rede



Bloquear o acesso a servidores de comando e controle



Usa dados de todos os serviços habilitados no Sophos Firewall

SOPHOS

Se você tiver um dispositivo comprometido em sua rede, a Proteção Avançada contra Ameaças, ou ATP, na Sophos Firewall pode ajudar a detectá-lo quando ele tenta entrar em contato com a Internet.

O ATP é uma configuração global que monitora o tráfego e os dados de todos os serviços habilitados no Sophos Firewall, incluindo solicitações DNS e da Web, para detectar e bloquear o acesso a servidores de comando e controle.

# Configuring Advanced Threat Protection

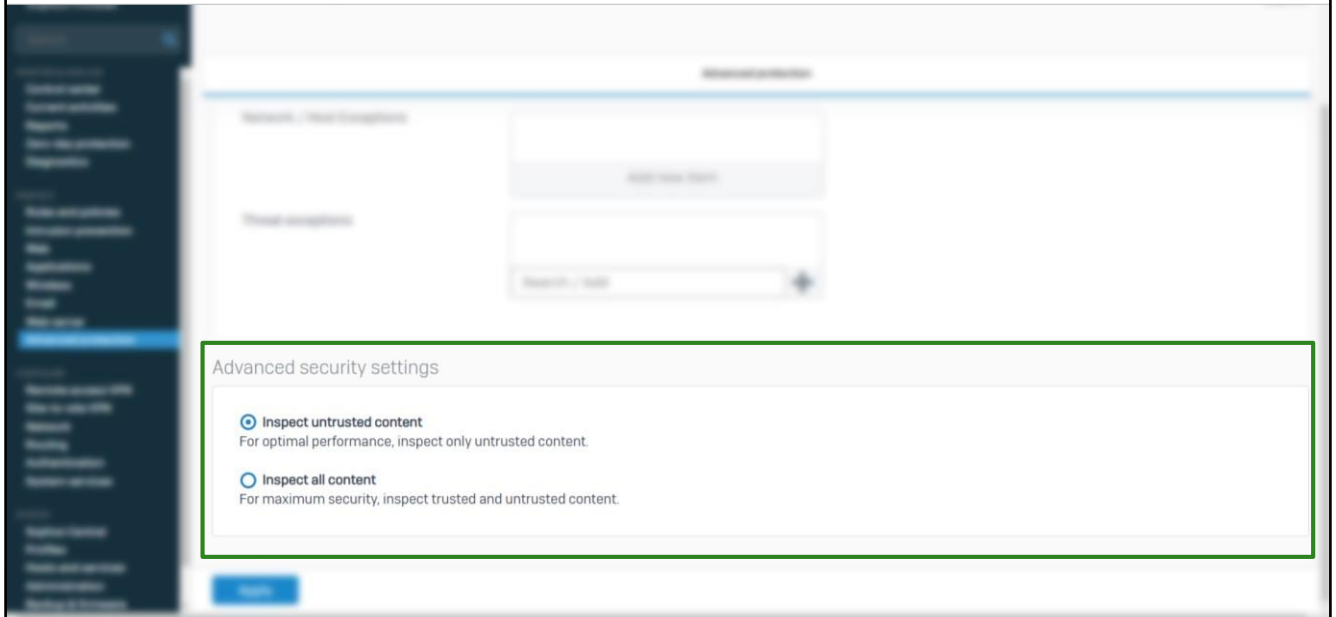
The screenshot shows the Sophos Firewall management interface. The left sidebar contains a navigation menu with categories: MONITOR & ANALYZE (Control center, Current activities, Reports, Zero-day protection, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, 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). The 'Advanced protection' option is highlighted. The main content area is titled 'Advanced protection' and includes a search bar, a 'Feedback' link, and a user profile 'admin@ny-gw.trainingdemo.xyz'. Below this, the 'Advanced threat protection' section is visible, featuring a toggle switch for 'Enable advanced threat protection' (set to ON), a 'Logging' section with an 'Enable' checkbox and a 'Change log settings' link, a 'Policy \*' dropdown menu (set to 'Log and drop'), and two empty lists for 'Network / Host Exceptions' and 'Threat exceptions'. Two green callout boxes are present: one pointing to the 'Policy \*' dropdown and another pointing to the 'Threat exceptions' list.

O ATP é configurado por meio de uma política simples em **PROTECT > Advanced protection**.

O ATP é habilitado usando o controle deslizante de alternância na parte superior da página. A política em si é uma escolha entre registrar apenas detecções de log ou registrar e descartar o tráfego.

O ATP é aplicado globalmente, portanto, se você precisar excluir dispositivos ou redes específicas, isso pode ser feito aqui. Você também pode optar por excluir ameaças específicas; no entanto, recomendamos que o faça apenas sob a orientação do apoio da Sophos.

# Configuring Advanced Threat Protection

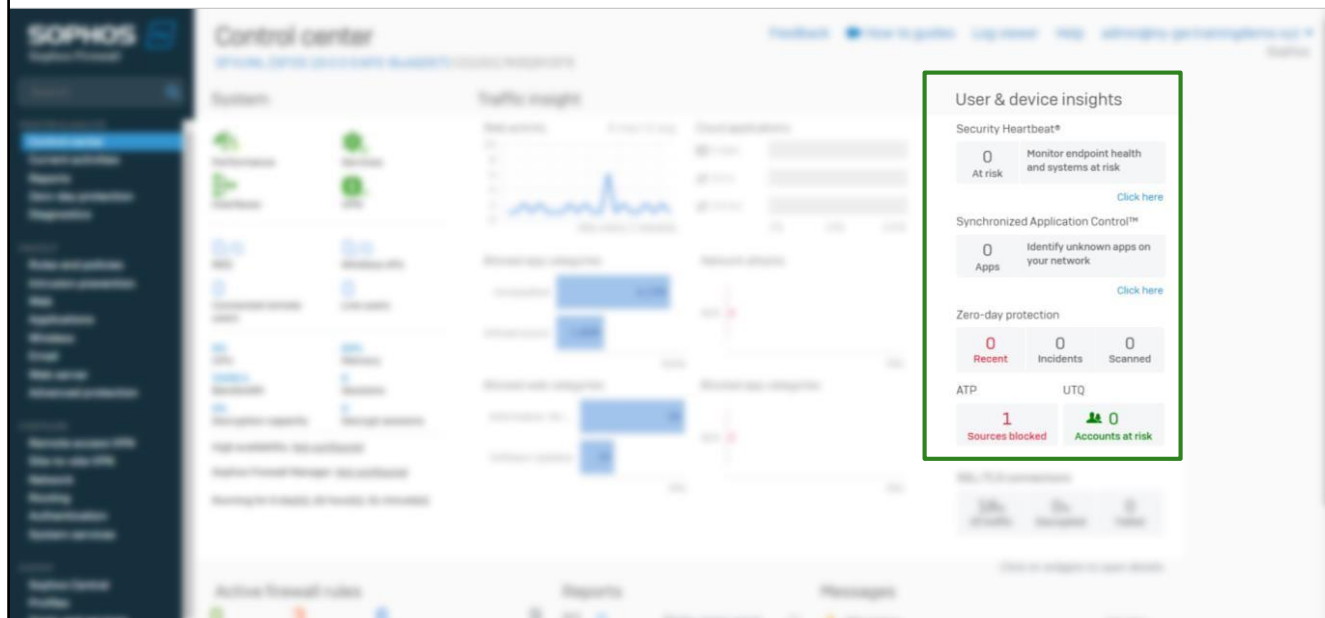


Na parte inferior da página está a seção "Configurações avançadas de segurança". Aqui você escolhe se o ATP inspeciona o conteúdo não confiável, essa é a opção padrão ou todo o conteúdo. Inspeccionar conteúdo não confiável inspeciona o tráfego de fontes não confiáveis ou o tráfego que vai apenas para destinos não confiáveis. Esta opção oferece o melhor desempenho.

Inspeccionar todo o conteúdo inspeciona todo o conteúdo de e para fontes e destinos confiáveis e não confiáveis.

Embora a diferença entre essas duas opções seja mínima, em ambientes de alto tráfego ela pode tornam-se significativos.

## Advanced Threat Protection Alerts



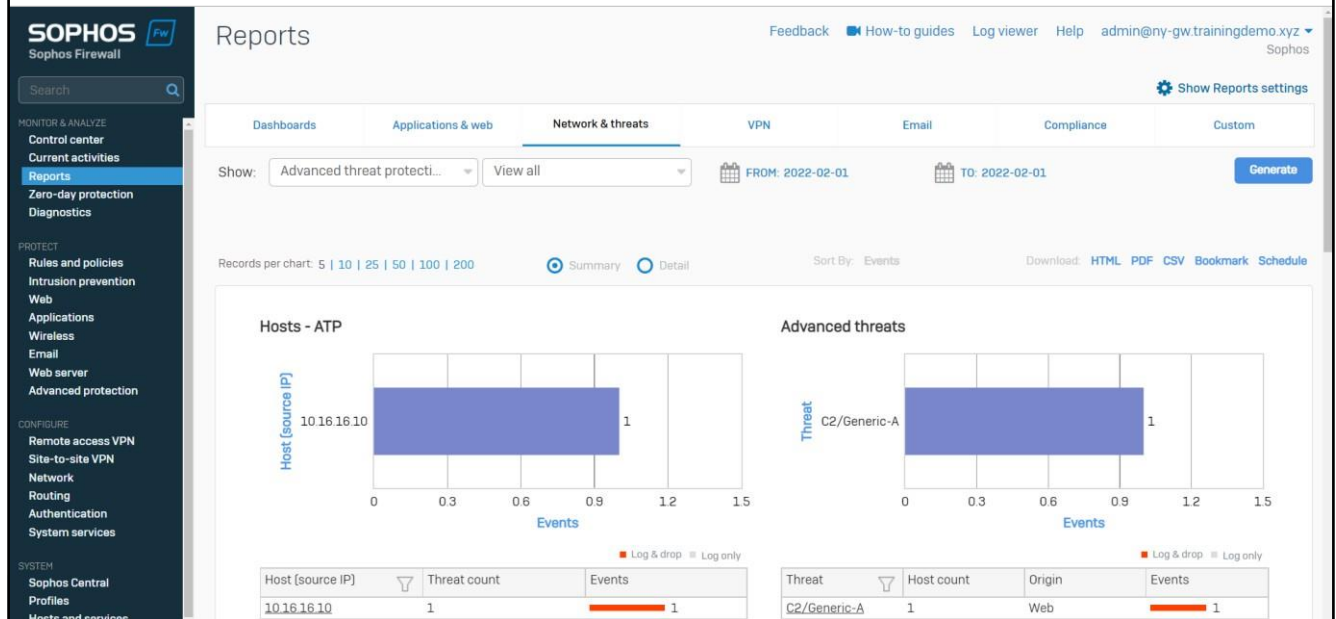
Há um widget para alertas ATP no centro de controle de firewall Sophos, que você pode clicar para obter informações adicionais.

# Advanced Threat Protection Alerts

The screenshot displays the Sophos Firewall Control Center interface. On the left is a dark sidebar with navigation menus: 'MONITOR & ANALYZE' (containing 'Control center', 'Current activities', 'Reports', 'Zero-day protection', and 'Diagnostics'), 'PROTECT' (containing 'Rules and policies', 'Intrusion prevention', 'Web', 'Applications', 'Wireless', 'Email', 'Web server', and 'Advanced protection'), 'CONFIGURE' (containing 'Remote access VPN', 'Site-to-site VPN', 'Network', 'Routing', 'Authentication', and 'System services'), and 'SYSTEM' (containing 'Sophos Central', 'Profiles', and 'Hosts and services'). The main panel is titled 'Control center' and shows the device 'SFVUNL (SFOS 19.0.0 EAP2-Build267) C010017K9Q8Y2F9'. A top navigation bar includes links for 'Feedback', 'How-to guides', 'Log viewer', 'Help', and a user profile 'admin@ny-gw.trainingdemo.xyz'. Below this, a tabbed interface shows 'SYSTEM', 'CPU & MEMORY', 'NETWORK', 'HEARTBEAT', 'ATP', 'RED', 'ALERT', 'CONNECTIONS & INTERFACES', and 'SSL/TLS INSPECTION'. The 'ATP' tab is active, displaying a summary card with a red '1' indicating 'Sources blocked' and a link to the 'ATP report'. Below the card is a table with columns 'HOSTNAME, IP', 'THREAT', and 'COUNT'. It lists one entry: IP '10.16.16.10' (Unknown hostname) with threat 'C2/Generic-A' (Unknown) and a count of '1'. A 'Reset' button is in the top right of the table area. At the bottom, there are three sections: 'Active firewall rules' with counts for WAF (0), User (3), Network (6), and Scanned (9); 'Reports' showing 'Risky apps seen' and 'Objectionable websites seen' (both 0 yesterday); and 'Messages' showing a 'Warning' about HTTPS/SSH management from 1m ago.

Depois de clicar no widget, você verá esta página que mostra as detecções, incluindo o endereço IP, nome do host e ameaça. Você pode clicar ainda mais nesta tela para o relatório ATP.

# Advanced Threat Protection Report



Você pode acessar o relatório ATP em **Reports > Network & threats**. Aqui você pode ver de onde as solicitações vieram e para onde elas estavam indo, quais usuários fizeram as solicitações e qual ação foi tomada, log ou log-and-drop.

## Simulação: Habilitando a Proteção Avançada contra Ameaças



Nesta simulação, você habilitará a proteção avançada contra ameaças, acionará uma detecção e revisará as informações resultantes.

SOPHOS

Nesta simulação, você habilitará a proteção avançada contra ameaças, acionará uma detecção e revisará as informações resultantes.