SOPHOS

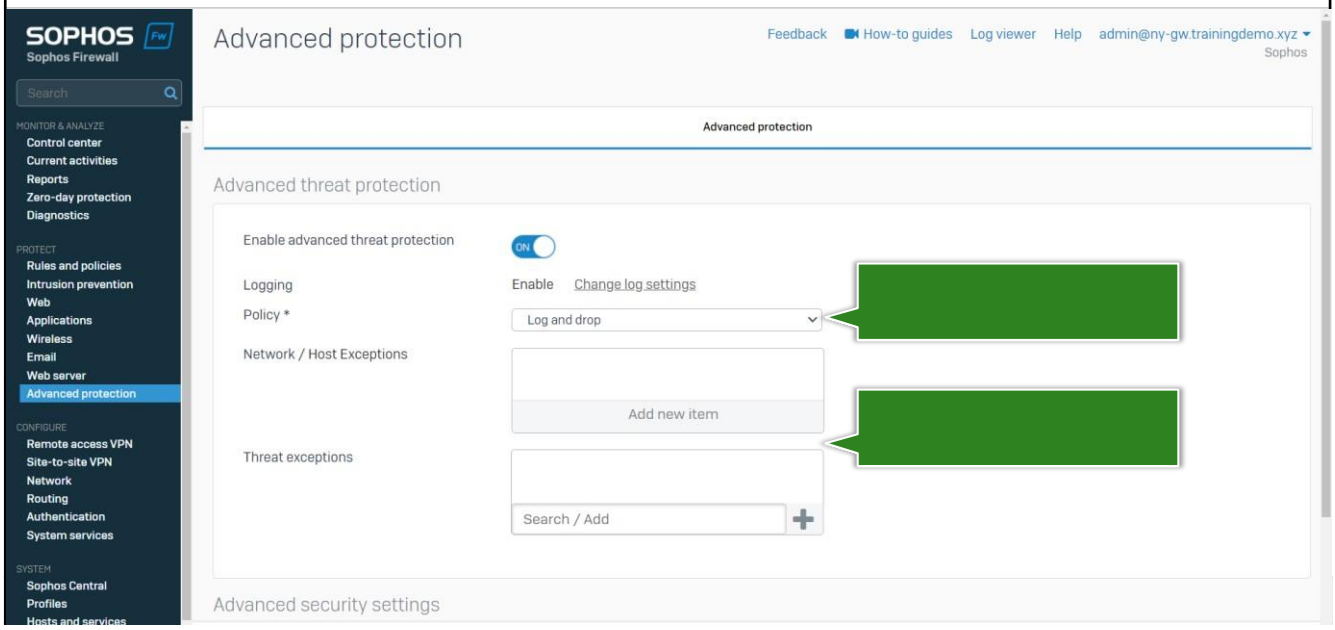
Enabling Advanced Threat Protection on Sophos Firewall

Sophos Firewall
Version: 19.0v1

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

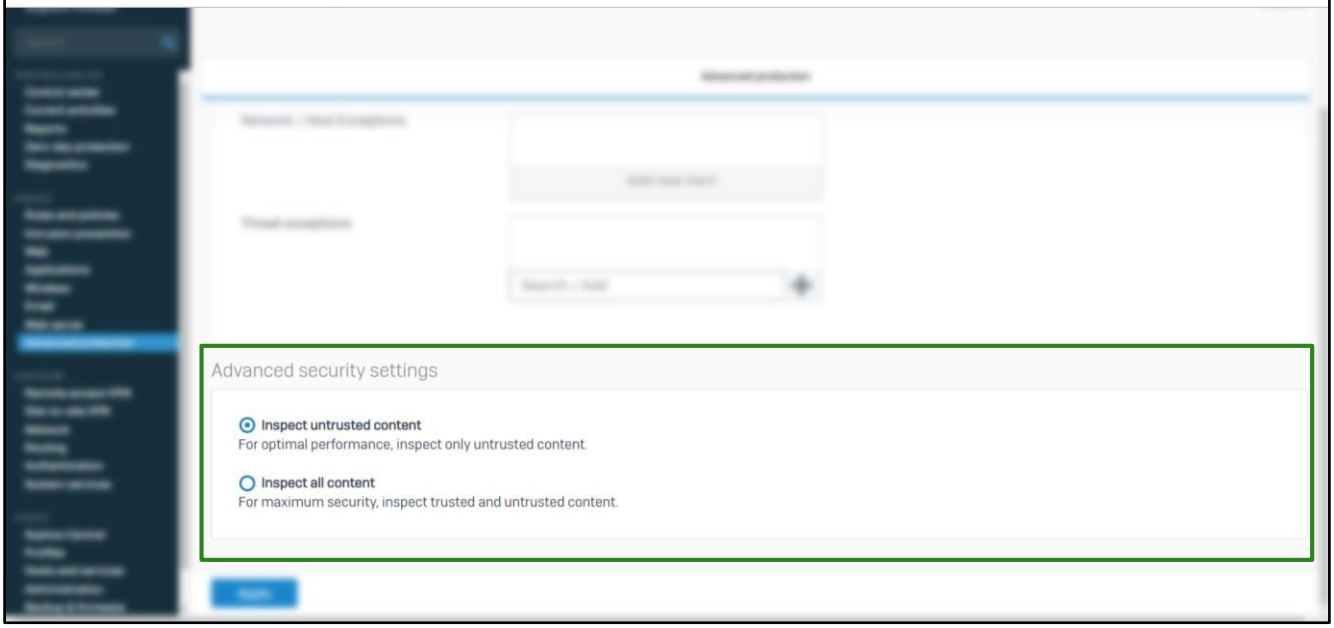


O ATP é configurado por meio de uma política simples em **PROTECT > Advanced protection**.

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

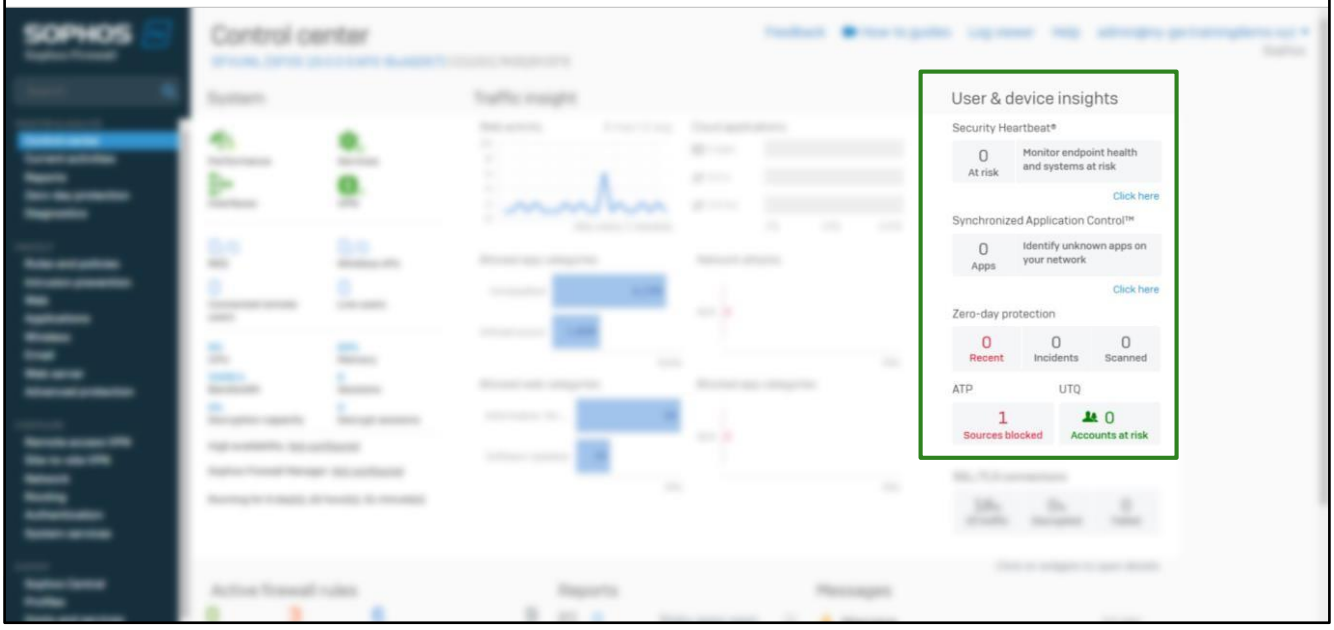


Na parte inferior da página está a seção "Configurações avançadas de segurança". Aqui você escolhe se o ATP inspeciona o conteúdo não confiável, essa é a opção padrão ou todo o conteúdo. Inspecionar conteúdo não confiável inspeciona o tráfego de fontes não confiáveis ou o tráfego que vai apenas para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

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

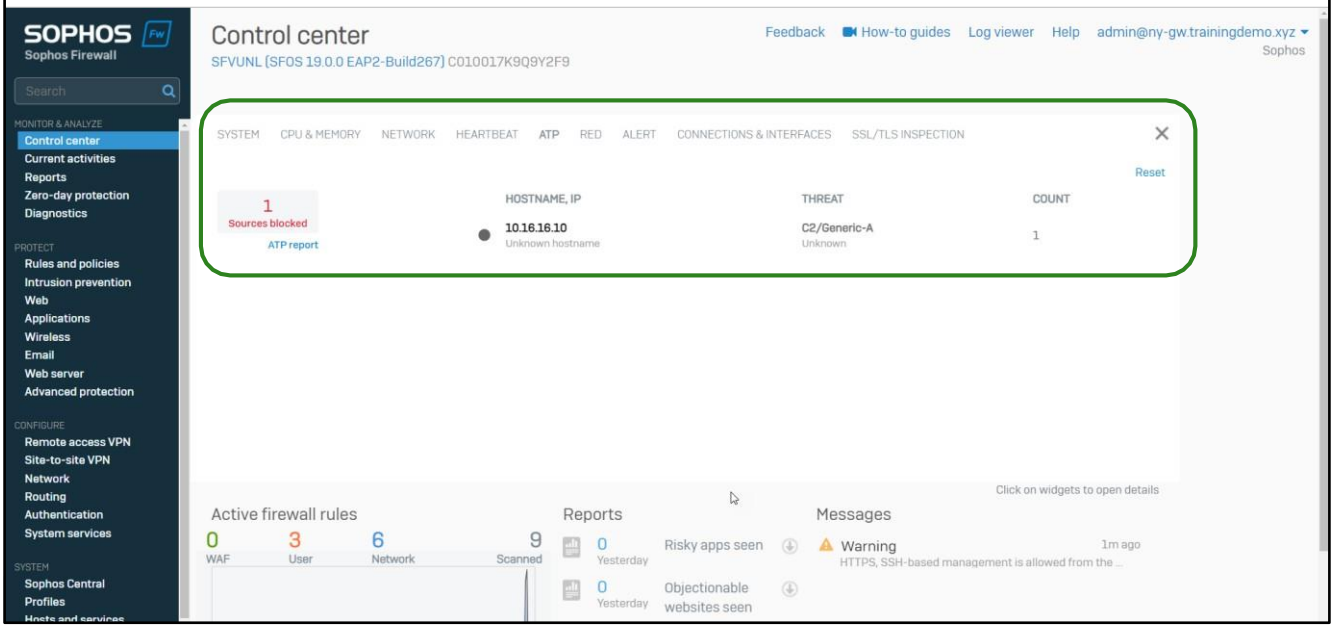
Embora a diferença entre essas duas opções seja mínima, em ambientes de alto tráfego ela pode tornam-se significativos.

Advanced Threat Protection Alerts



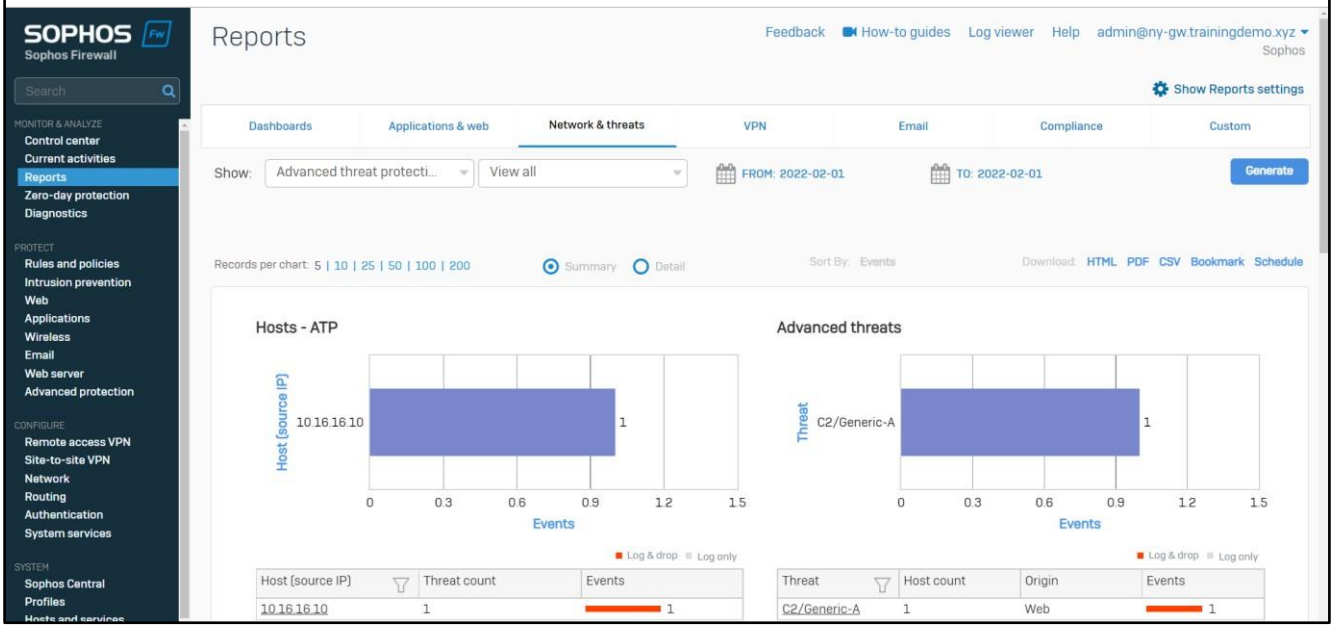
Há um widget para alertas ATP no centro de controle de firewall Sophos, que você pode clicar para obter informações adicionais.

Advanced Threat Protection Alerts

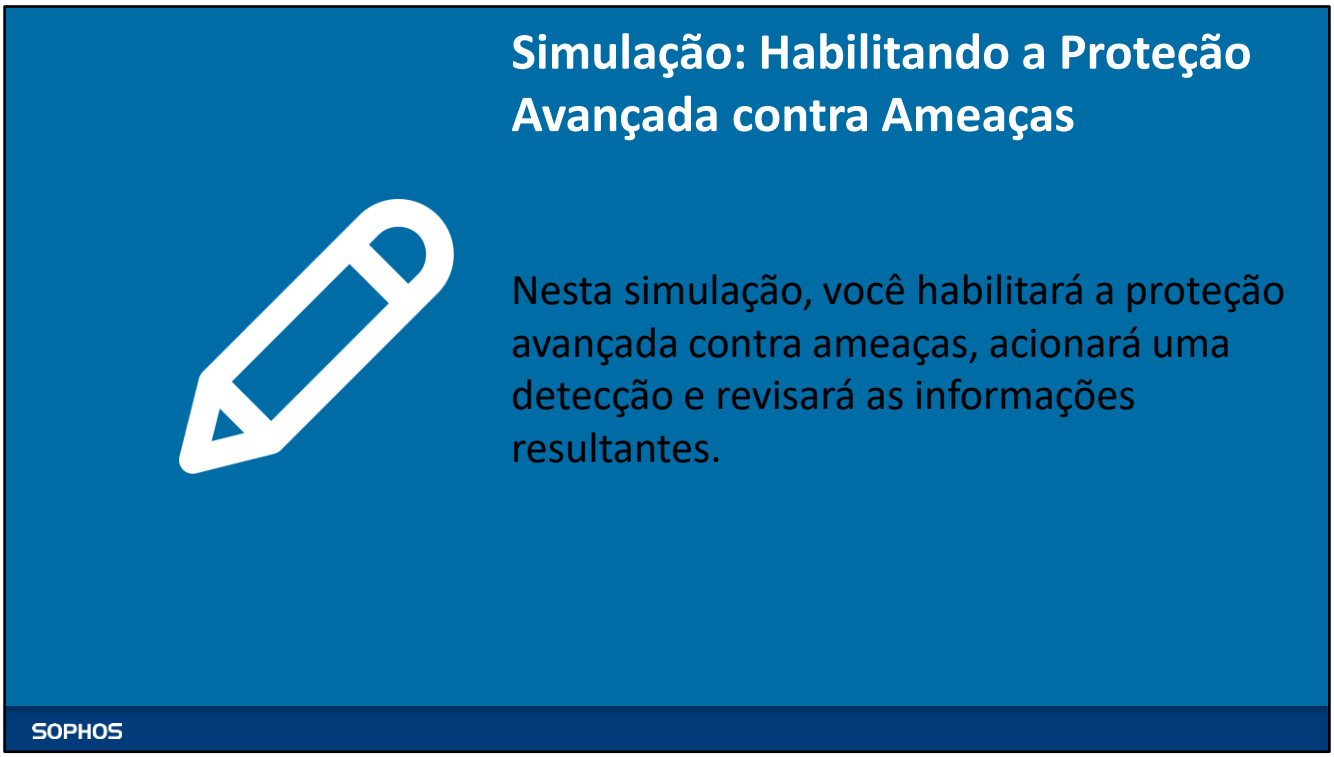


Depois de clicar no widget, você verá esta página que mostra as detecções, incluindo o endereço IP, nome do host e ameaça. Você pode clicar ainda mais nesta tela para o relatório ATP.

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.



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