Boas Práticas

Web Protection (Proteção da Web)

N-able N-sight RMM

Sumário

Introdução

Este documento tem como objetivo abordar a configuração do recurso **Web Protection** de forma segura e evitando erros, como também fornecer familiaridade com a ferramenta e os conceitos envolvidos, baseando-se no ambiente a ser instalado.

Assim como qualquer outra solução a implementação e configuração do **Web Protection** exige planejamento e compreensão do ambiente como um todo e também da ferramenta em si. Portanto sempre utilize o **manual do N-able N-sight RMM (sessão do Web Protection)** para orientações.

É necessário que você, enquanto prestador de serviço, entenda que o **Web Protection** envolve uma série de responsabilidades como gestão, configuração, controle e manuseio.

Vale ressaltar também a importância do registro de acessos nos relatórios da solução, como um acompanhamento diário.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para **boaspraticas@addee.com.br**.

1. Pré-Requisitos

+ URLs de Comunicação

Além das **URLs do N-able N-sight RMM** e das **URLs e Portas do Agente de Monitoramento**, é necessário incluir essas URLs abaixo na lista de permissões do seu software de Firewall:

api.bcti.brightcloud.com
echo-us-west-2-block.logicnow.us
echo-us-west-2-svc.logicnow.us
echo-logicnow-us-prod.s3.amazonaws.com
echo-logicnow-us-prod.us-west-2.s3.amazonaws.com
s3-us-west-2.amazonaws.com/echo-logicnow-us-prod
echo-logicnow-us-repdb.s3.amazonaws.com
echo-logicnow-us-repdb.us-west-2.s3.amazonaws.com
s3-us-west-2.amazonaws.com/echo-logicnow-us-repdb
s3-us-west-2.amazonaws.com/echo-logicnow-us-usage

+ Permissões do Usuário no N-sight RMM

A instalação e configuração do Web Protection dependem dos privilégios do usuário e de sua função de conta no N-sight RMM. Para ter acesso as configurações o usuário precisa ser pelo menos do nível superusuário ou administrador (não clássico).

+ Soluções Concorrentes

Antes de instalar o **Web Protection** no dispositivo verifique se não há nenhuma outra solução ativa no mesmo, que esteja fazendo o mesmo trabalho de filtragem de rede. Alguns antivírus possuem tal recurso e mantê-lo ativado pode causar problemas na funcionalidade do **Web Protection**.

Portanto para que o **Web Protection** tenha uma melhor eficácia é preciso ser a única ferramenta de filtro de rede ativa no dispositivo.

2. Pré-Ativação

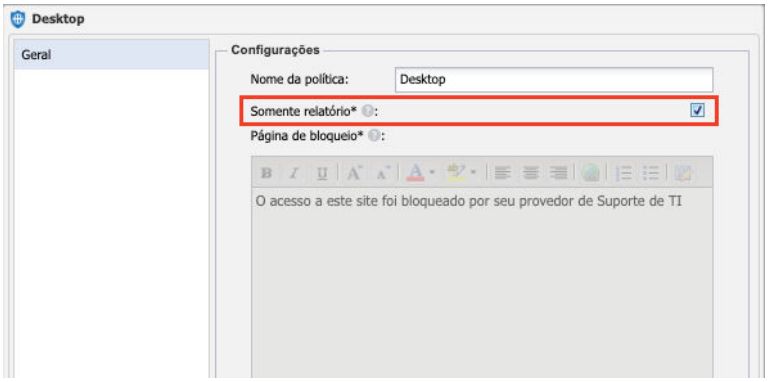
Antes de tudo, é bom relembrar que o **Web Protection** oferece como primeiro foco a **segurança na Web** e como segundo foco a **filtragem dos dados**. Portanto, assim que você habilita o recurso e utiliza uma das políticas padrões da ferramenta a segurança na Web já está sendo realizada, independente de ter ou não ter feito a configuração inicial de filtragem dos dados.

Ao ativar o Web Protection pela primeira vez, a nossa sugestão de uso é que seja ativada a opção Somente Relatório, mesmo sem ter realizado nenhuma configuração de filtragem. Desta forma será possível avaliar quais são as URLs e conteúdos mais acessados pelos dispositivos e posteriormente realizar o planejamento de configuração de bloqueio/liberação da política.

Observação: A utilização no modo **Somente Relatório** por uma semana é suficiente para coletar as informações de uso, e os relatórios do recurso **(explicados posteriormente no passo 6)** fornecerão as informações sobre a utilização Web.

Para habilitar o modo **Somente Relatório** em uma política do **Web Protection** faça o seguinte:

1. Acesse o menu Configurações / Web Protection / Política de Proteção;
2. Crie uma nova política com nome “Somente Relatório”;
3. Edite esta política e, em Geral, marque somente a checkbox Somente Relatório, conforme a imagem abaixo:



4. Salve a política somente com esta configuração.

Observação: Utilize esta política sempre que for ativar o **Web Protection** em um novo cliente primeiramente, onde você precisará levantar os dados iniciais antes de aplicar as configurações necessárias.

Assim que obtiver todas as informações, crie uma nova política com as parametrizações necessárias para aquele ambiente e aplique-a no(s) dispositivo(s) Cada cliente pode possuir a sua própria política de filtragem dos dados interna, seja ela geral para os seus devices, separadas por setor ou individualmente, máquina por máquina.

Criando uma política de proteção específica para aquele cliente (ou site ou dispositivo) além de você atender as necessidades dele você conseguirá elaborar o teu próprio padrão de organização e controle das políticas, facilitando uma possível alteração futura.

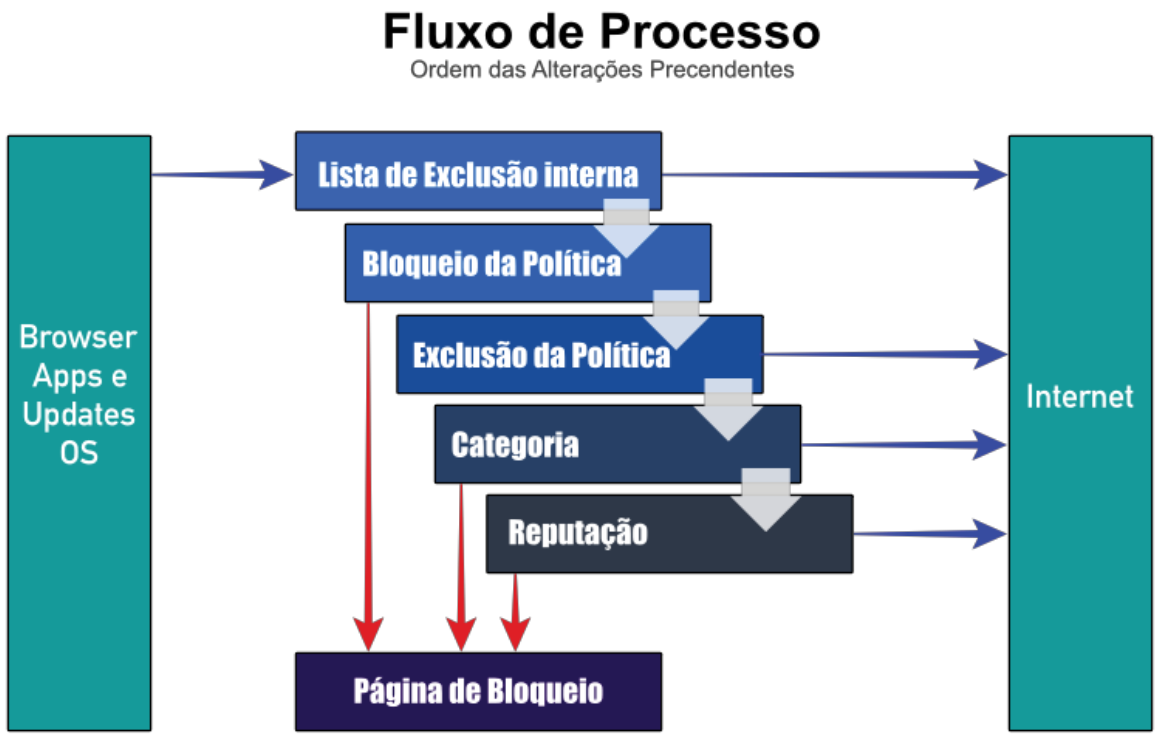
Entretanto, não se esqueça de que, quanto mais políticas diversificadas criadas maior será o trabalho do MSP em geri-las, numa possível alteração ou até mesmo na criação das mesmas.

Após avaliar o relatório gerado durante esta primeira semana, **crie uma nova política** e aplique as filtragens na política de proteção conforme avaliado com o cliente.

3. Política de Proteção

Assim como os outros recursos do N-able N-sight RMM o Web Protection também é configurado através de uma política de proteção, na qual você pode customizá-las e separá-las por clientes ou dispositivos.

Mas antes de falarmos sobre a política de proteção, veja na imagem abaixo que o Web Protection obedece a seguinte ordem de fluxo de processo para realizar os bloqueios/liberações:



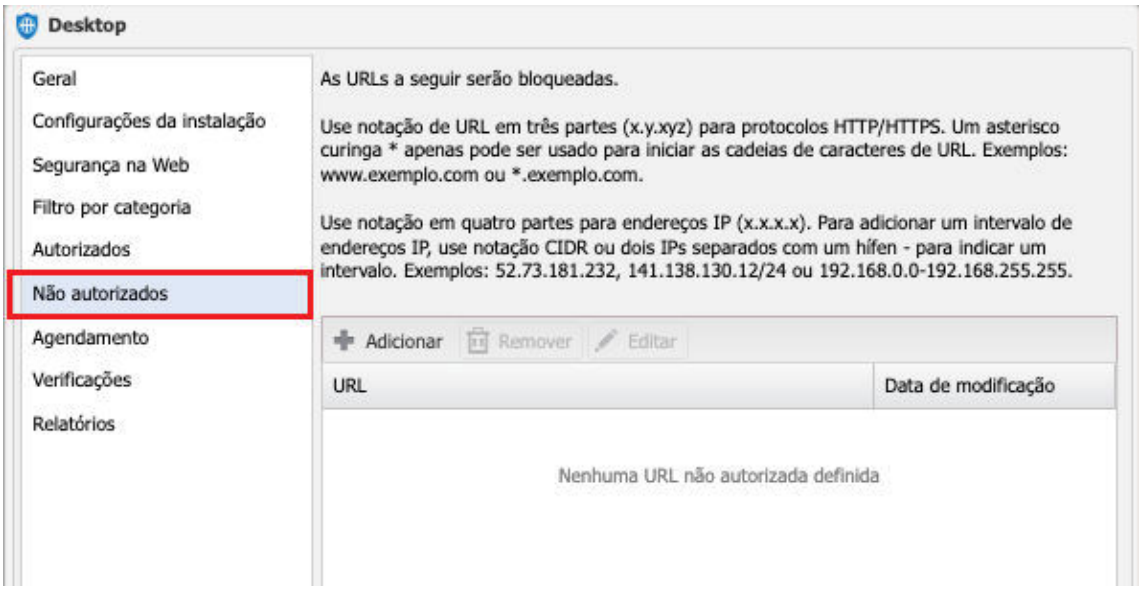
Repare que existe no topo da lista a "**Lista Interna de Sites Permitidos**", que é uma whitelist da própria **Webroot**, no qual é administrada pela mesma.

Isto significa que apenas habilitando a política do **Web Protection**, mesmo sem aplicar nenhuma configuração de bloqueio, seja por site, categoria ou reputação, a política já fará o bloqueio de sites maliciosos e indesejados por padrão, garantindo a sua segurança na rede.

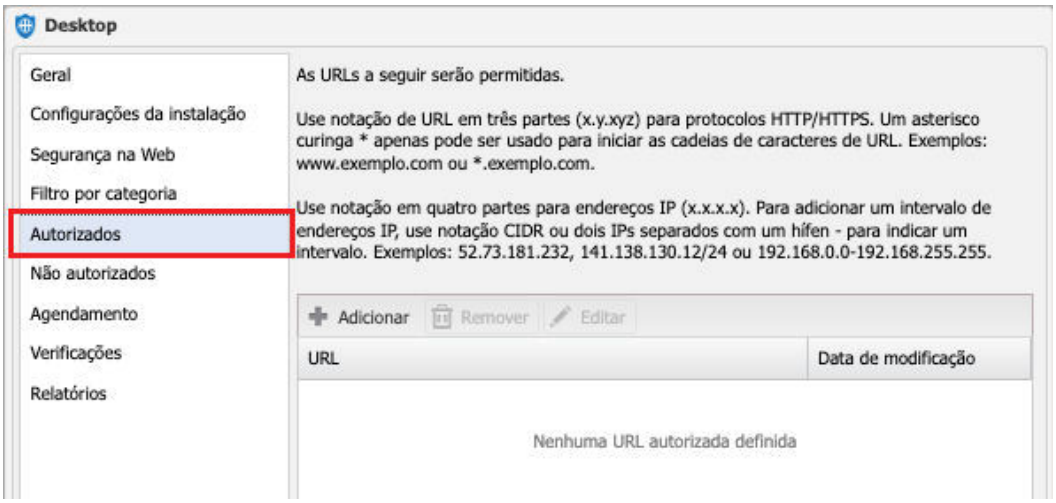
Observação: Uma vez que o site a ser acessado está bloqueado por esta lista interna é necessário entrar em contato com a **Webroot**, através do site deles **(https://www.brightcloud.com/tools/url-ip-lookup.php)** para solicitar a inclusão deste site da lista interna de sites permitidos, ou até mesmo a alteração da reputação ou categoria em que estão enquadrados.

No caso da alteração, a solicitação passará por uma análise da **Webroot** e, em caso de aprovação, a reputação/categoria será alterada.

Na sequência existe o "**Bloqueio da Política**" que é a blacklist definida na política do Web Protection. Todos os sites inseridos na aba "**Não Autorizados**", na política, não serão acessados pelo dispositivo, independente da categoria ou reputação em que eles se encontram, até mesmo se estiverem sido inseridos na aba "**Autorizados**".

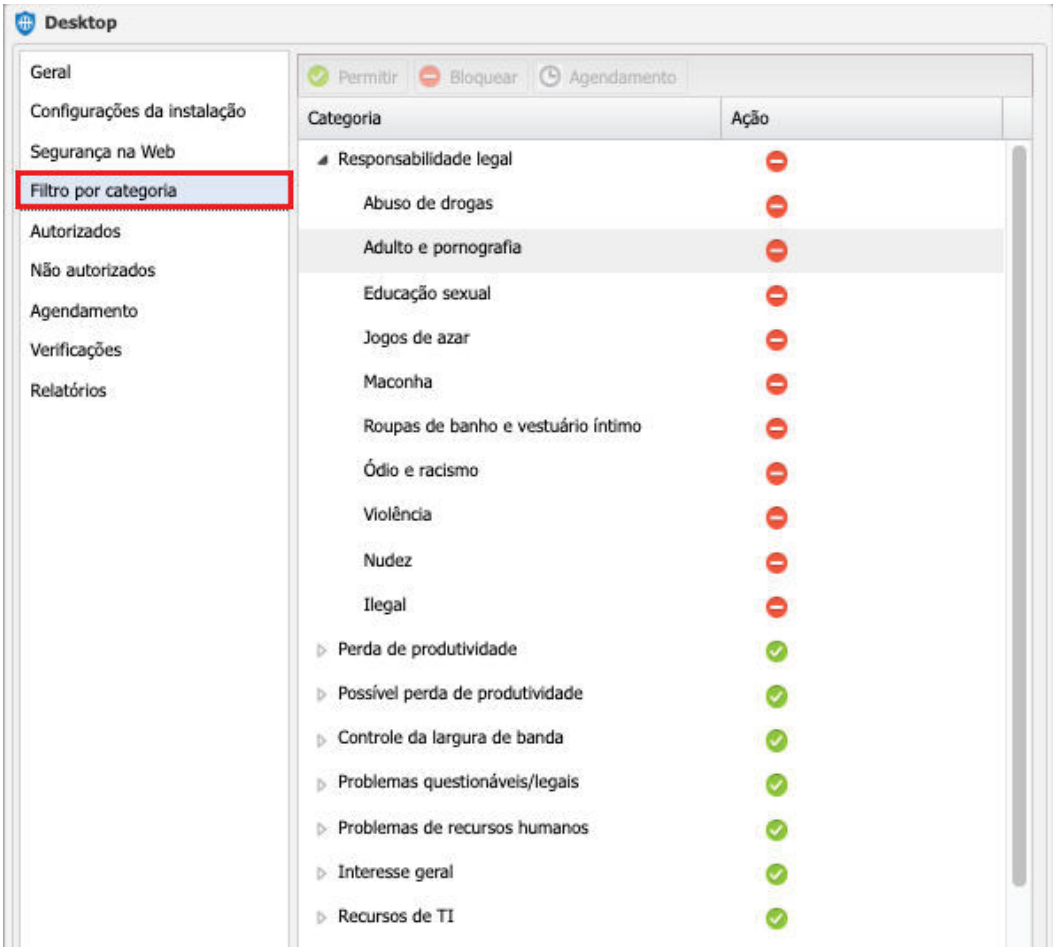


Em seguida temos, também dentro da política do **Web Protection**, a "**Exclusão da Política**", que é representada pela aba "**Autorizados**". Portanto se a reputação ou a categoria do site está bloqueada, mas o site se encontra dentro da aba "**Autorizados**", o acesso ao site será permitido.

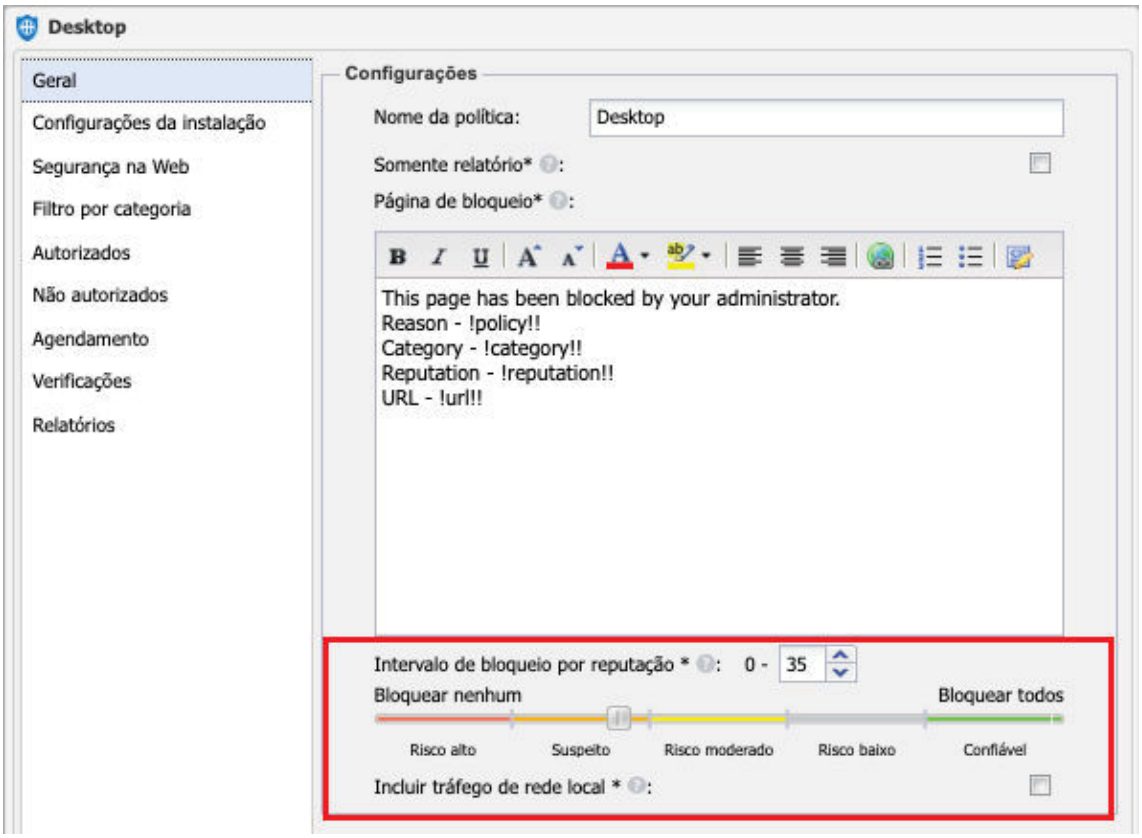


Observação: Note que a blacklist possui prioridade em relação a whitelist, ou seja, se uma URL estiver na blacklist e também na whitelist a mes ma será bloqueada por conta desta regra.

Já em "**Categoria**", a política do **Web Protection** permite filtrar sites pela categoria em que o site está enquadrado, permitindo, bloqueando ou agendando o acesso.



Em “Reputação”, é possivel definir o bloqueio dos sites pelo nível de reputação em que eles estão enquadrados, sendo de Risco Alto (0 - 19) até Confiável (81 - 100).



Observação: Por padrão, e por motivos de segurança, sites com reputação de Risco Alto (abaixo de 20) são bloqueados diretamente pela Webroot.

Para acessar a política de proteção do **Web Protection** vá em: **Configurações / Web Protection / Política de Proteção**

+ Aba GERAL – Interação com o Usuário Final

Nesta parte da configuração temos estas duas checkbox abaixo que podem facilitar a identificação dos sites e subsites que estão sendo acessados naquele momento.

Marcando a opção Mostrar Ícone na Barra de Tarefas o Web Protection irá registrar, através do ícone, os sites e domínios acessados, juntamente com as mensagens e avisos de bloqueio ao usuário. Isto não é feito como notificação, ou seja, será necessário abrir este ícone para ter acesso as informações.

E marcando a opção Mostrar Notificações será gerado um alerta no canto da tela com o resumo das informações da mensagem, a cada nova mensagem gerada e gravada no ícone.

+ Aba GERAL - Intervalo de Bloqueio por Reputação

Este intervalo de bloqueio por reputação, por padrão da N-able, vem marcado para bloquear sites de reputação **Risco Total (0 – 19) e Suspeito (20 – 39)**. O MSP pode aumentar ou diminuir este controle por reputação, conforme sua necessidade.

Desta forma o **Web Protection** bloqueará acesso aos sites com a reputação abaixo deste valor (lembrando que sites com reputação abaixo de 19 são bloqueados automaticamente pela Webroot, mesmo se estiver configurado para não bloquear este nível de reputação na política).

Alguns sites utilizam subsistes durante a navegação, no qual estes podem se enquadrar em uma reputação que esteja definida para bloquear. Neste caso o MSP precisa se atentar ao endereço que o site está tentando acessar para verificar sua reputação e liberar teu acesso, se for o caso.

Para consultar a reputação do site, utilize o recurso **Pesquisa de Sites**, localizado no **N-Sight RMM**. Para isto, acesse o menu: **Configurações / Web Protection / Pesquisa de Sites**.

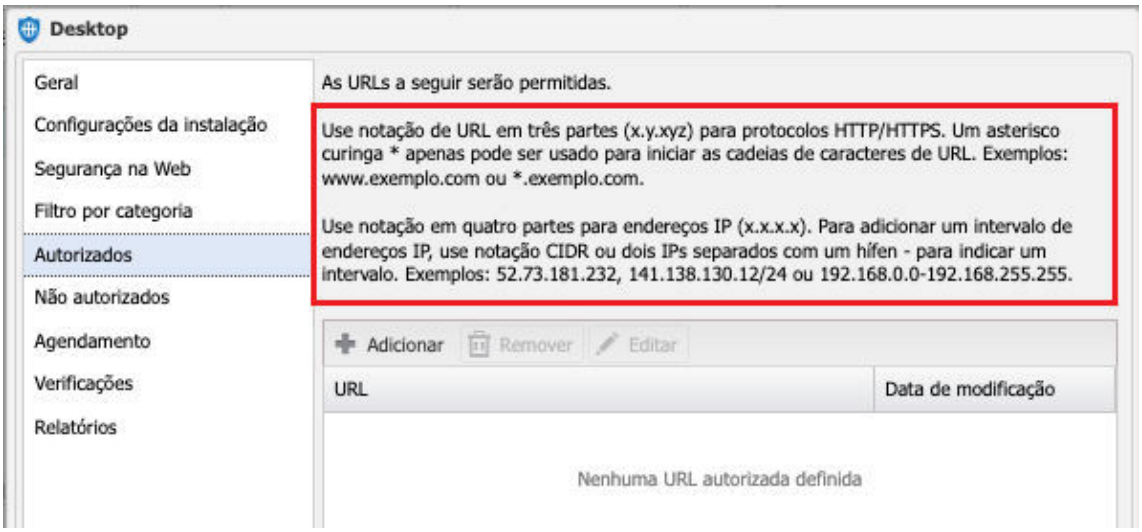
+ Aba FILTRO POR CATEGORIA

Assim como a reputação, todo site possui a sua categoria que também pode ser configurada para bloquear. Se o site se enquadrar em alguma categoria bloqueada o site não será exibido, independente da reputação estar liberada ou não.

Para consultar a reputação do site, utilize o recurso **Pesquisa de Sites**, localizado no **N-Sight RMM**. Para isto, acesse o menu: **Configurações / Web Protection / Pesquisa de Sites**.

+ Abas AUTORIZADOS e NÃO AUTORIZADOS

Sempre que precisar adicionar um site na whitelist ou na blacklist utilize o **coringa asterisco (*)**, seguindo as orientações do manual descrito na própria janela, para garantir que o prefixo ou o sufixo utilizado seja autorizado ou não autorizado para acesso.



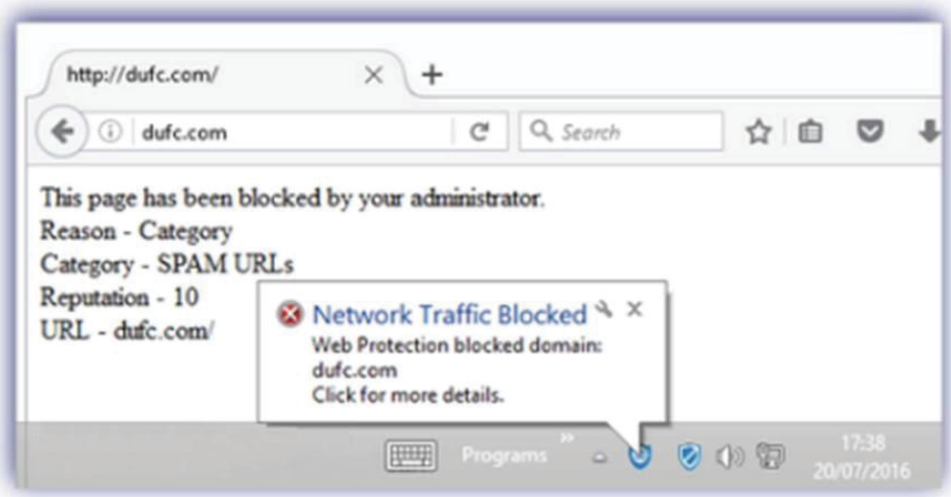
Inclua sempre o nome do site e todos seus subsites ou variações da URL possíveis, para evitar que o site seja acessado utilizando outros protocolos ou outros prefixos.

4. Ícone Barra de Tarefas

O **Web Protection** permite habilitar um ícone na barra de tarefas do dispositivo monitorado, que não apenas informa ao cliente que o Web Protection está sendo executado como também fornece algumas informações sobre os sites, sub sites e domínios acessados (categoria e reputação, por exemplo), juntamente com as informações do bloqueio de acesso ao site.

As configurações "**Mostrar ícone da barra de tarefas**" e "**Mostrar notificações**" são definidas nas configurações política (aba Geral) e, quando habilitadas, exibirão uma notificação (ou informação) quando um site for bloqueado.

Por exemplo, a notificação **Trafego de Rede Bloqueado (Network Traffic Blocked)**, quando exibida na tela, informa qual é o domínio bloqueado (neste exemplo, "dufc.com") e também inclui uma opção "**Clique para mais detalhes**", no qual abrirá a **Console de Notificações do Web Protection**.

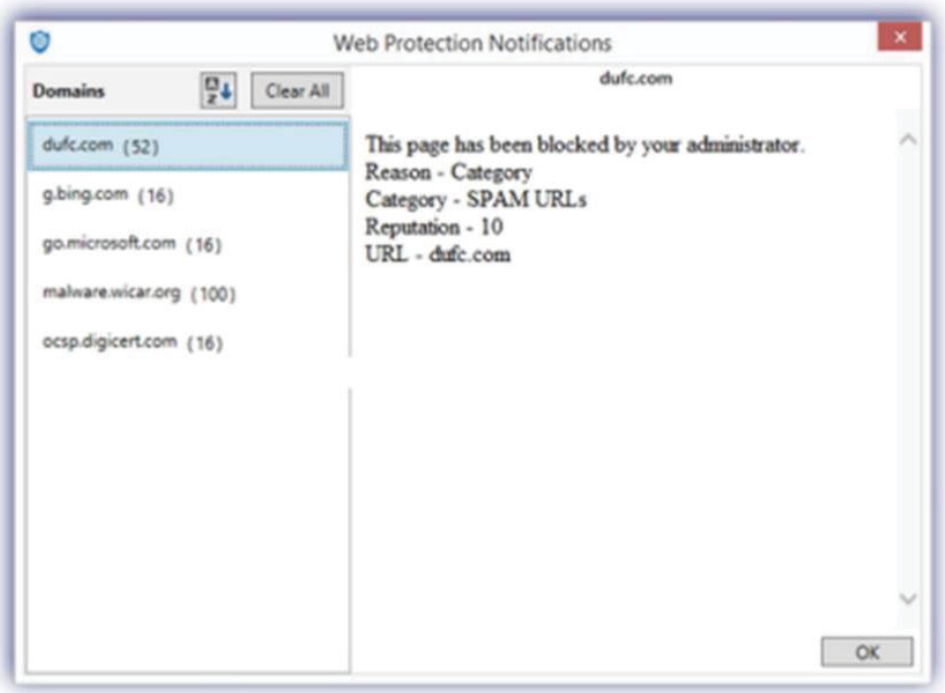


Nela você encontrará informações sobre os domínios bloqueados no painel esquerdo da tela, junto com a opção de classificar em ordem alfabética e limpar todas as notificações na exibição da console.

+ Console de Notificações Web Protection

Com o recurso do ícone do Web Protection ativado é possível acessar a Console de Notificações para poder visualizar em tempo real qual ou quais são os domínios, sub sites, recursos e extensões que estão sendo acessados por determinado site bloqueado.

Ou seja, caso você queira saber quais os recursos que um determinado site utiliza (seja eles domínios ou sub sites) assim que ele é acessado você pode verificar todas estas informações nesta console.



A console ainda conta com o recurso de limpeza de registro (botão “Clear All”) que permite que você exclua todos os registros anteriores e foque somente nos novos acessos.

Esta ferramenta é muito útil para ser utilizada quando se pretende liberar algum site “teimoso”, onde mesmo adicionando na parte de “Autorizados” ele continua bloqueando o acesso.

Sabendo disto, caso você precise realizar alguma liberação de um site no Web Protection você pode usar a Console de Notificações como aliada, seguindo este pequeno passo-a-passo abaixo que elaboramos para auxílio:

1. Habilite o ícone da barra de tarefas do Web Protection na política de proteção utilizada para este dispositivo;

2. Abra o navegador de internet e mantenha apenas uma aba limpa aberta. Se houver outro navegador aberto ou outras abas do navegador abertas é recomendável encerrar ou fechá-las;

3. Abra a Console de Notificações do Web Protection (clicando sobre o ícone da barra de tarefas) e limpe todos os registros já gravados inicialmente (botão “Clear All”);

4. Volte para o navegador e acesse somente o site que pretende liberar (que esteja bloqueado);

5. Abra novamente a Console de Notificações do Web Protection e veja quais foram os domínios acessados, do lado esquerdo da tela. Estes domínios você vai precisar incluí-los na lista de sites liberados na política de proteção do recurso.

5. Problemas Comuns

As causas de falhas durante a instalação ou utilização do **Web Protection** podem variar e cada uma requer um procedimento específico para correção. Abaixo listaremos as mais comuns:

+ Instalação - Falha na Captura de Rede

Para corrigir o erro de instalação "**Falha na Captura de Rede**" faça o seguinte procedimento no dispositivo local:

- No Windows, em "**Central de Rede e Compartilhamento**", acesse a opção **Configuração dos Adaptadores de Rede** e, por fim, **desative o IPv6** nas interfaces ativas.

- É importante que o Windows esteja atualizado, então certifique-se de que o Sistema Operacional está com todas as atualizações em dia.

- Após isto, desative e ative o recurso no painel novamente para que uma nova instalação seja feita, e o recurso identifique as alterações realizadas.

+ Sites não estão sendo bloqueados

Caso você esteja tentando bloquear um site e mesmo inserindo-o na aba "**Não Autorizados**" ele continua sendo acessado normalmente, cheque os seguintes pontos abaixo:

- **Verifique as configurações da política deste device:** Certifique-se de que o site foi inserido corretamente na aba "**Não Autorizados**", da mesma forma como é digitado no navegador. Você também pode optar por utilizar o **coringa (*)** no prefixo ou sufixo do site, para validar.

- **Limpe os caches e cookies do navegador:** Uma vez que um site é acessado o navegador salva os dados daquele site em forma de cache com a intenção de ajudar com o consumo da largura de banda.

Desta forma, da próxima vez que o site for reaberto ele levará menos tempo para ser carregado, pois uma versão em cache da página já foi salva no dispositivo.

Portanto, ao aplicar um bloqueio na política do **Web Protection** para um determinado site sempre opte por limpar os caches e cookies do navegador, ou até mesmo os registros gravados somente deste site, para ter certeza de que estes dados salvos não serão mais utilizados, invalidando a nova configuração da política.

- **Utilize uma janela anônima ou outro navegador:** Como teste você também pode abrir uma nova janela anônima do navegador e tentar acessar o site.

Se o site não abrir normalmente (e a política de bloqueio aparecer) você saberá que há algo neste navegador que está permitindo o acesso (caches, cookies, extensões, configurações internas, etc.).

Por padrão os recursos anônimos dos navegadores não carregam e não gravam informações em caches ou cookies, que são salvos nos dispositivos, portanto é um bom teste inicial a ser realizado.

- **Desabilite o Protocolo IP Versão 6 (TCP/IPv6):** Este protocolo, quando habilitado, pode causar incompatibilidade com o **Web Protection** no bloqueio de determinados sites.

Para desabilitá-lo, acesse **Painel de Controle \ Rede e Internet \ Conexões de Rede**. Clique com o botão direito na rede em que está conectado e selecione "**Propriedades**".

Localize a opção "**Protocolo IP Versão 6 (TCP/IPv6)**" e desmarque-a. Clique em OK para salvar as alterações.

- **Desabilite o QUIC Protocol no Google Chrome:** O **QUIC** é um protocolo de comunicação criado para permitir mais rapidez na transferência e dados.

Devido a esta rapidez na transferência o **Web Protection** pode não conseguir bloquear alguns sites no Google Chrome.

Para desabilitar acesse "chrome://flags" (sem as aspas), localize o "**Experimental QUIC protocol**" e desabilite-o.

+ Não Aparece a Página de Bloqueio

Este problema ocorre porque o site acessado está utilizando o **protocolo HTTPS**. Todos os sites que utilizam este protocolo HTTPS permitem serem bloqueados pela ferramenta, porém alguns destes protocolos não retransmitem a página de bloqueio definida no **Web Protection**, trazendo em seu lugar uma página em branco, com a mensagem de que a página não pode ser exibida, ou um erro de SSL.

Devido a isto o **Web Protection** não consegue mostrar a página de bloqueio, mas o site está bloqueado, e não será possível acessá-lo.

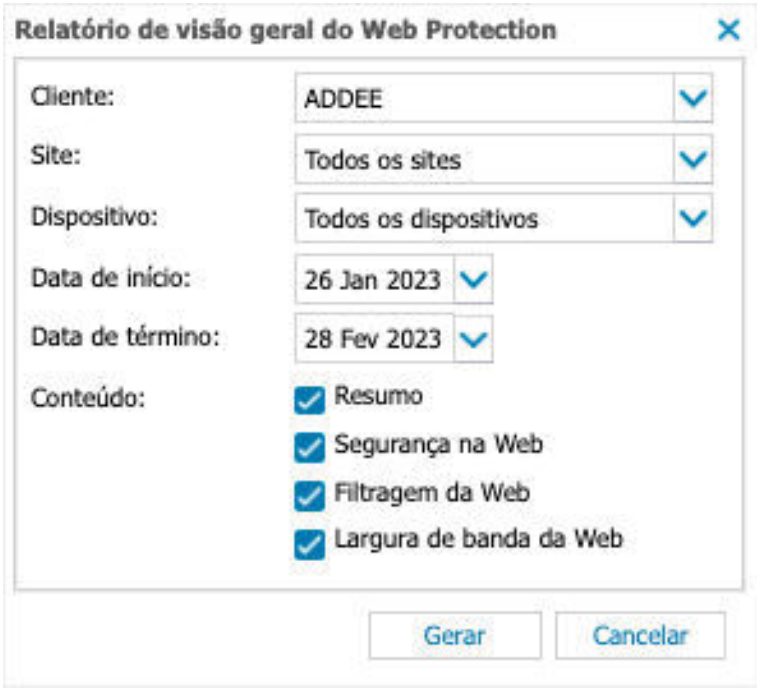
6. Relatórios

Além das informações contidas na aba Web, no painel Sul do **N-sight RMM**, para um determinado dispositivo, é possível obter relatórios das informações captadas pelo **Web Protection**.

O **N-able N-sight RMM** disponibiliza 2 relatórios para o Web Protection:

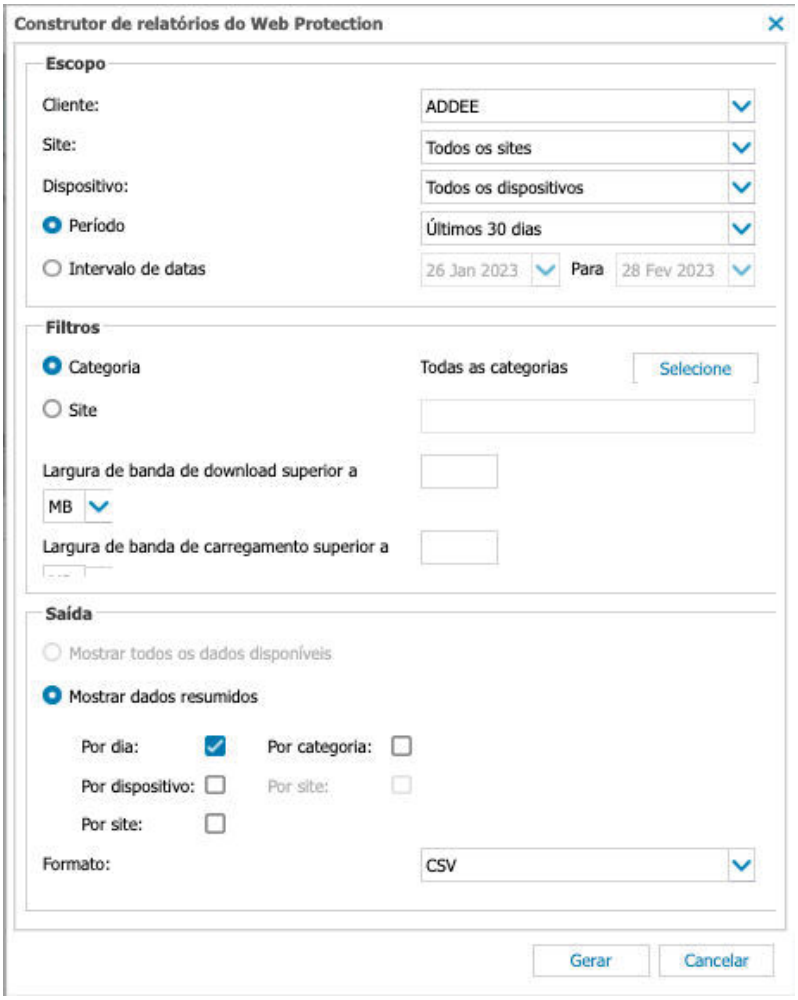
- **Relatório de Visão Geral:** Neste relatório é possível ter uma informação detalhada sobre as atividades realizadas nos dispositivos de um determinado cliente, trazendo em seu conteúdo um resumo sobre os acessos, informações sobre a segurança na Web, filtragem da Web e largura de banda da Web.

Também permite filtrar as informações por Cliente, Site e Dispositivo, com um **período máximo de até 30 dias passados**.

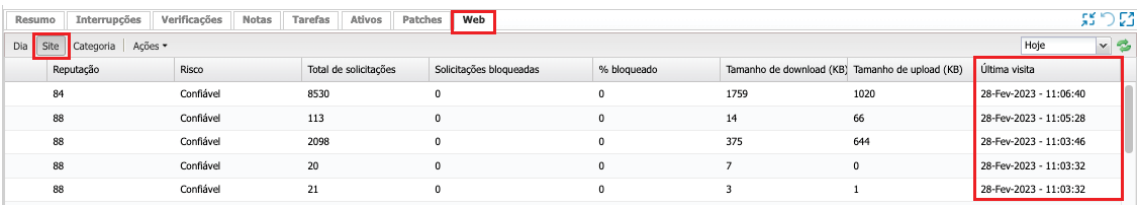


- **Construtor de Relatório:** Neste outro relatório é possível montar um relatório semelhante ao **Relatório de Visão Geral**, porém, mas com algumas opções de informações a mais.

Filtragem por categoria, por site ou por largura de banda, dados completos ou resumidos por dia, por dispositivo, por site ou por categoria e também contém a possibilidade de extração do relatório via formato **CSV** ou **HTML**.



Observação: Nenhum relatório do **Web Protection** mostrará o horário exato que tal site foi acessado. Porém na aba Web, sub aba Site, é possível verificar através da coluna "última visita" qual foi o último momento em que o site teve acesso.



7. Log Verbose

Em alguns casos será necessário avaliar os registros da ferramenta para identificar o motivo do site estar ou não estar liberado, uma vez que todas as configurações acima já foram revistas.

O **Web Protection** conta com um tipo de log diferente para registrar tais informações chamado de **log Verbose**. Este log é essencial para a análise realizada pelo nosso desenvolvimento.

Então caso seja necessário entrar em contato com o suporte da ADDEE para verificar o motivo do site não estar bloqueado (ou liberado) você pode antecipar a coleta deste log, realizando os seguintes passos abaixo:

- No dispositivo afetado, abra o **CMD** como administrador e digite o seguinte comando para habilitar a captura do log: "**C:\Program Files\Advanced Monitoring Agent Web Protection\webprotection.exe**" verbose

- Reproduza o problema (acesse o site).

- Vá em "**C:\ProgramData\AdvancedMonitoringAgentWebProtection**" e envie o arquivo **AdvancedMonitoringAgentWebProtection.log** pelo ticket aberto para análise do suporte **ADDEE**.

- Após isto, abra novamente no **CMD** como administrador e digite o seguinte comando para desabilitar a captura do log: "**C:\Program Files\Advanced Monitoring Agent Web Protection\webprotection.exe**" noverbose

Observação: É importante **desabilitar o log verbose** após o uso para que o agente não continue gerando logs de acesso, consumindo um espaço desnecessário no HD.

Empresa brasileira, iniciamos nossas operações em 2013 com o objetivo de revolucionar o mercado de Prestação de Serviços de TI e contribuir com o enriquecimento moral, intelectual e financeiro de nossos clientes e colaboradores.

Nascemos da necessidade de um Prestador de Serviços de TI e hoje somos Distribuidores das melhores ferramentas para Prestadores de Serviços de TI de todo o Brasil.

Trabalhamos para o crescimento sustentável do mercado de tecnologia, através do compartilhamento de conhecimentos e a distribuição de soluções inovadoras para Gestão de TI. Com estrutura local, fornecemos atendimento e suporte em português, além de todo o apoio comercial necessário para empresas de Serviços de TI.

Compreendemos as necessidades locais e por isso somos o principal parceiro de negócios dos nossos clientes.

Com um time de profissionais altamente qualificados e apaixonados por tecnologia e relacionamento, colocamos acima de tudo, as pessoas. É assim que fazemos negócios.

Última alteração: Março/2023

Responsável: Caio Gutierri

E-mail: boaspraticas@addee.com.br

YouTube Instagram Linkedin Site Blog