GUIA DE CONFIGURAÇÃO

CONTROLE DE APLICAÇÕES

GUIA DE CONFIGURAÇÃO – CONTROLE DE APLICAÇÕES

1. Next Generation Firewall: uma explicação simples

Com o avanço que a WEB 2.0 trouxe ao mundo digital, práticas até então pouco exploradas como a interação online, a colaboração e redes sociais têm nos aproximado cada vez mais do conceito da WEB 3.0. Aplicações que até então estávamos acostumados a utilizar somente em redes locais (LAN), iniciaram um processo de migração para o conceito de nuvem, trazendo benefícios que nos dão a certeza de ser uma tendência que veio para ficar.

Além disso, aplicações online que julgávamos ser de uso exclusivo para interações pessoais, como por exemplo Facebook, Twitter e YouTube se tornaram ferramentas indispensáveis no mundo corporativo. Empresas migraram seus canais de atendimento online para o Twitter, passaram a utilizar o Facebook como site corporativo, migraram seus serviços de e-mail para o Gmail e começaram a utilizar o Youtube como portal de vídeos corporativos.

Se voltarmos para o mundo de segurança da informação, uma preocupação que as equipes de TI tinham era a de buscar ferramentas e/ou equipamentos capazes de bloquear exatamente as aplicações citadas acima, com a justificativa de aumentar a produtividade de seus funcionários e melhorar a segurança de suas redes. Hoje em dia, bloquear tais aplicações se tornou um verdadeiro problema, pois passou a afetar os negócios da empresa.

A grande diferença entre um firewall tradicional e um Next Generation é capacidade de filtragem e correlacionamento entre os indicadores de ameaças (conteúdo proibido ou malicioso, malwares, aplicativos não permitidos), além da forma como o administrador indica o que pode ou não pode ser feito. No Next Generation Firewall a configuração das regras e políticas de segurança é feita de uma forma diferente, que torna o trabalho do administrador mais intuitivo e simples.

No firewall tradicional as regras são baseadas principalmente nos parâmetros do TCP/IP: endereço de origem e destino, tipo de protocolo, porta, etc. Tudo isso é uma linguagem técnica complexa, que exige um bom conhecimento de redes por parte dos administradores.

Cabe ao administrador compreender como cada protocolo funciona e criar uma regra. Além de trabalhoso é algo que exige mais experiência do administrador. Além disso, muitas empresas sofrem com falta de profissionais capazes de manter apropriadamente as regras.

Por outro lado, a forma como se acessa a Internet está mudando. Por questão de redundância e eficiência um mesmo site fica hospedado em vários servidores espalhados pela Internet (diversos endereços IPs) e um site pode conter serviços importantes e inúteis/perigosos ao mesmo tempo (ex.: Facebook pode conter informações importantes sobre concorrentes para comparação e ao mesmo tempo jogos que apenas distraem o usuário).

Um outro problema é que estão surgindo aplicações cujo objetivo é driblar essas regras de firewall, usando as regras permitidas como brecha para acessar serviços não permitidos.

O grande efeito prático é que custa caro para as empresas (salário de profissionais ou valores de consultoria) manterem os firewalls tradicionais funcionando apropriadamente e mesmo assim nem sempre estão conseguindo implementar uma política adequada.

Dessa forma os Next Generation Firewall chegam para resolver esses problemas.

Em primeiro lugar o administrador de um Next Generation Firewall não precisa mais saber a porta TCP ou endereço IP de um serviço. O Next Generation Firewall "conhece" os serviços e permite ao administrador liberar ou não baseado no nome desses serviço.

Por exemplo, um administrador quer liberar acesso ao Linkedin e aos sites corporativos do Facebook, mas quer proibir jogos do Facebook. Para isso o administrador indica "liberar Linkedin", "liberar Facebook corporativo", proibir "Facebook jogos". O Next Generation Firewall conhece todos esses serviços e já tem pronta as regras.

Além disso o Next Generation Firewall inspeciona todos os pacotes, procurando por mecanismos que tentem burlar as regras.

Outra característica do Next Generation Firewall é a capacidade de identificar cada usuário, independentemente de onde ele esteja e de qual equipamento esteja utilizando (hoje em dia é comum o mesmo usuário se conectar na rede através do seu computador, tablet e smartphone, tudo ao mesmo tempo). Assim o Next Generation Firewall identifica o usuário (e não apenas o seu endereço IP) para saber o que ele pode ou não fazer.

Em resumo, o Next Generation Firewall é mais simples de configurar. Sendo mais simples ele acaba trazendo algumas vantagens importantes:

- a empresa não necessita de um profissional tão especializado. Isso significa redução de custos em consultorias ou certificação de pessoal.
- por "absorver" as complexidades cada vez maiores dos tipos de acessos feitos pelos usuários.

Unindo isso tudo ao fato dele identificar claramente cada usuário temos uma solução mais apropriada ao ambiente corporativo.

2. Inspeção profunda de pacotes (Deep Packet Inspection)

A DPI (inspeção profunda de pacotes) é uma tecnologia usada para capturar pacotes de rede à medida que passam por roteadores e outros dispositivos de rede, além de realizar uma filtragem de pacotes para examinar os dados e localizar informações mais profundas sobre os dados levados pelos pacotes.

Ao contrário da inspeção dinâmica de pacotes (SPI, também conhecida como inspeção superficial de pacotes), que somente verifica o cabeçalho o u o rodapé de um pacote, a DPI examina o cabeçalho, o rodapé, a origem e o destino dos pacotes recebidos, e os dados que são parte do pacote, pesquisando por instruções ilegais e critérios predefinidos, correlacionando-os, permitindo que você decida ou não se permite que o tráfego passe por meio de sua rede.

A DPI faz com que seja possível localizar, identificar, classificar, redirecionar ou bloquear pacotes e ajuda você a determinar – com base no conteúdo que está nos pacotes de dados – se o tráfego é seguro, compatível, permitido e realmente necessário para o aplicativo do usuário final/ponto de extremidade ou não.

Algumas aplicações importantes da DPI

- Perícia detalhada do tráfego de rede para auxiliar a análise baseada no fluxo
- Monitoramento de desempenho de rede baseado em aplicação
- Reconhecimento de aplicação baseada em rede
- Regulamentação e controle do tráfego de rede
- Segurança de rede (para identificar vírus, spams e intrusões)

Diferença entre análise de fluxo e DPI

A análise de tráfego de rede baseada em fluxo permite que você intercepte o fluxo de tráfego de rede à medida que ele passa pelos dispositivos de rede habilitados para o fluxo (roteadores e interruptores). A análise de fluxo fornece dados abrangentes para validar a qualidade de serviço, o tipo de serviço e a classe de serviço do pacote de rede, sua origem e endereço IP de destino etc.

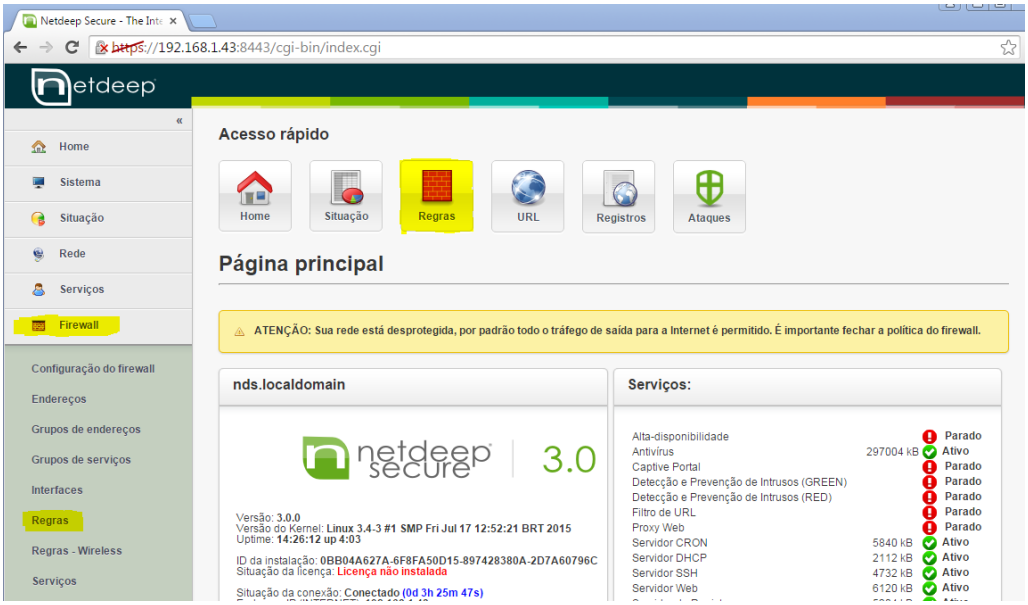
A DPI realiza a filtragem e a investigação forense profunda do pacote e examina cada parte de todos os pacotes que passam por meio da inspeção da DPI. A DPI tem a capacidade de inspecionar o tráfego em camadas de 2 a 7, permitindo que você obtenha informações detalhadas de qual conteúdo (não somente o tipo de conteúdo, mas o próprio conteúdo) está passando pela sua rede.

O Netdeep Secure 3.0 vem com este recurso e você pode criar regras de firewall baseadas nas assinaturas das aplicações. Acompanhe os passos a seguir.

IMPORTANTE: Os filtros criados funcionam independentemente dos módulos de Proxy Web e Filtro de URL estiverem habilitados.

3. Bloqueando/liberando aplicações

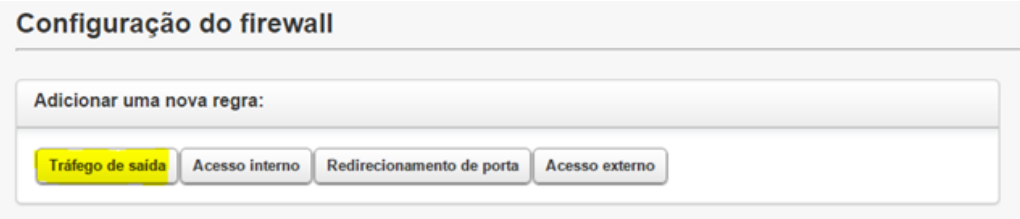
Para poder realizar esta configuração, navegue até a interface de administração do Netdeep Secure, vá ao menu "**Firewall**" → "**Regras**" ou então, utilizando a guia **Acesso rápido** clique no botão "**Regras**".



Você pode criar aplicar o filtro de aplicações na maioria dos tipos de regras: **Tráfego de Saída, Acesso Interno, Tráfego Interno e Acesso externo.**

Neste exemplo, iremos ensinar como configurar o bloqueio da saída. **Isto é, o sistema filtrará a conexão de saída para a Internet.**

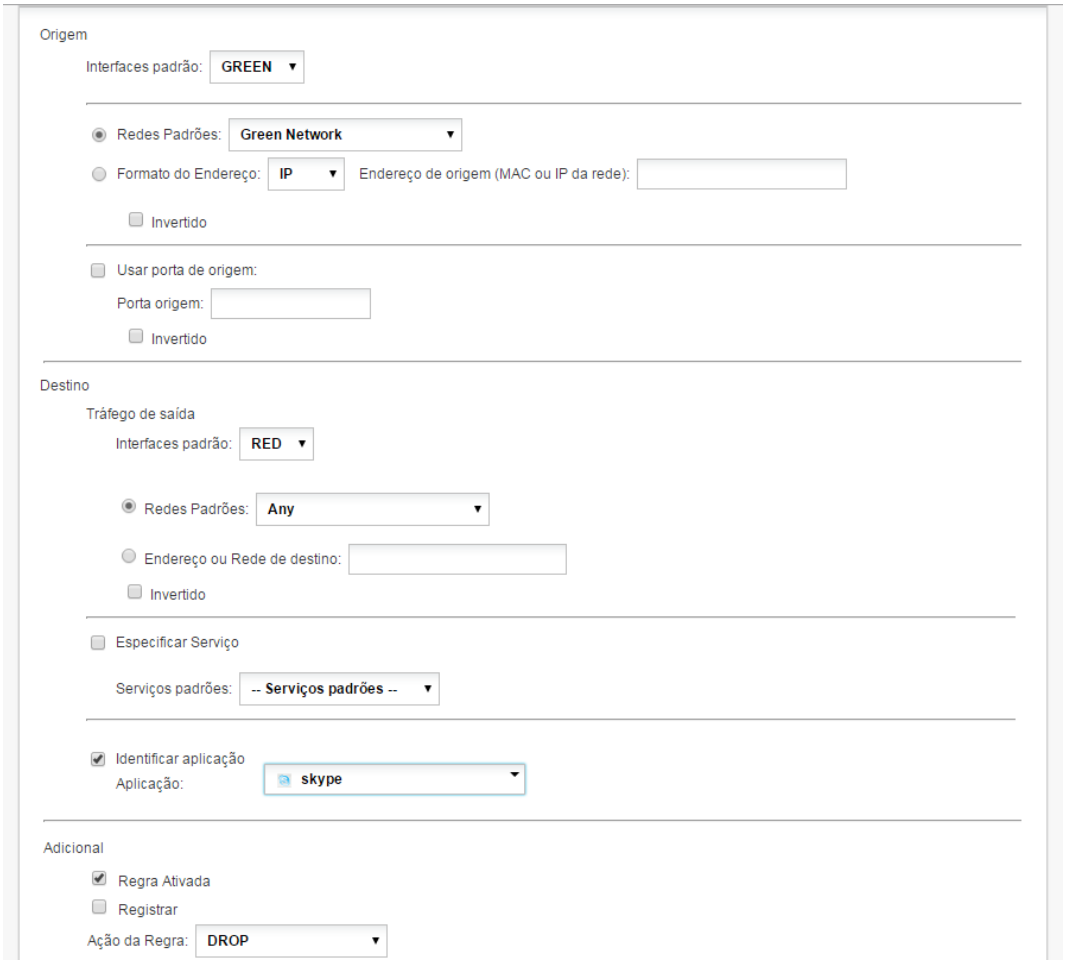
Para criar uma regra de tráfego de saída, na caixa “Adicionar uma nova regra”, clique no botão “**Tráfego de saída**”.



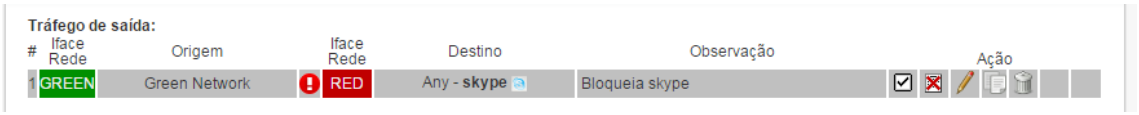
Em **Origem** iremos deixar a “Interfaces padrão” como **GREEN** (rede interna), em “Redes Padrões”, você pode especificar qual a rede será usada, ou especificar um endereço personalizado. Neste exemplo, iremos filtrar toda a rede interna, selecionando **Green Network.** Em “Usar porta de origem” deixar desabilitado.

Em **Destino** iremos deixar a “Interfaces padrão” como **RED** (interface de acesso a Internet), em “Redes Padrões” **Any** (qualquer endereço). Caso queira reforçar ainda mais a segurança, você pode escolher um serviço e dentro dele especificar para identificar aplicação. Em nosso exemplo não iremos fazer isso. Então desmarque a opção “Especificar Serviço” e marque a opção “Identificar aplicação” e em seguida selecione a aplicação. Neste exemplo, iremos bloquear o **skype**.

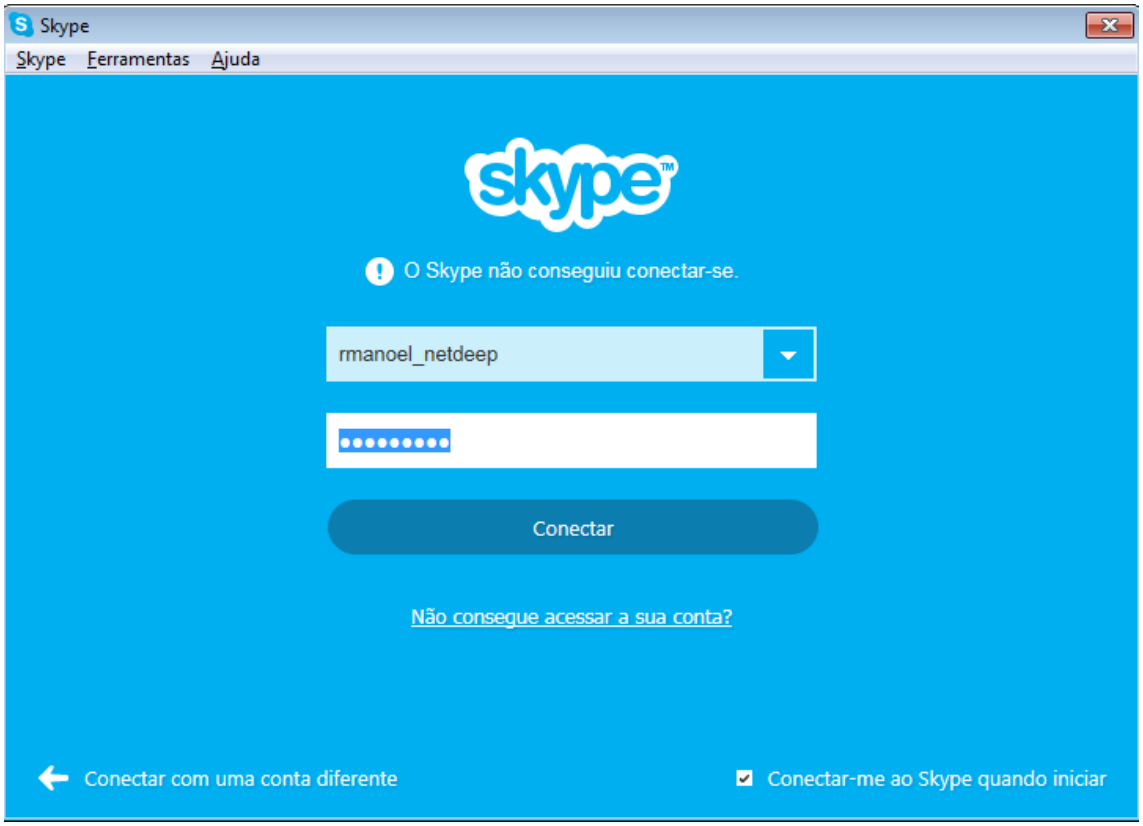
Em **Adicional** certifique-se que a opção “Regra Ativada” esteja marcada e em seguida em “Ação da Regra” escolha a opção **DROP**. No campo “Observação” coloque um pequeno texto informando o que a regra faz, por exemplo, “**Bloqueia skype**” e em seguida clique no botão **Salvar**.



A regra deverá estar como a figura abaixo, caso estiver diferente favor verificar os passos acima novamente.



Tentativa de se conectar ao skype depois que a regra foi criada.

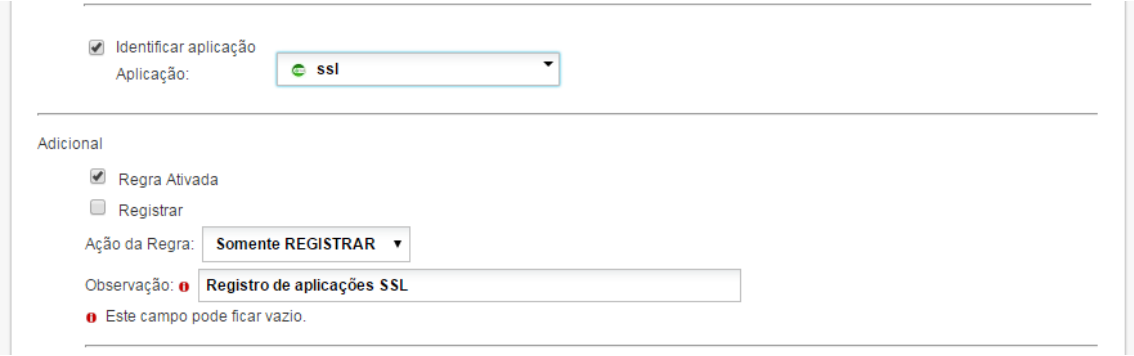


4. Bloqueando/liberando aplicações que utilizam criptografia SSL

Existem alguns aplicativos que são criptografados por SSL (os que usam HTTPS por exemplo). Para identifica-los é necessário adicionar primeiramente uma regra para registrar as aplicações SSL. Isto é válido por exemplo para Facebook, Twitter, Youtube, Gmail.

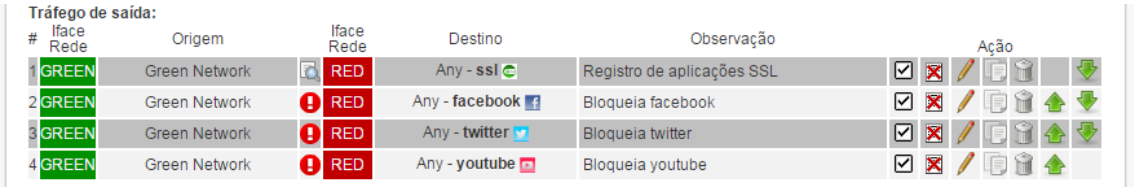
Neste exemplo, vamos criar uma regra para bloqueio do Facebook. Para isso clique no botão "**Tráfego de saída**".

Utilize o mesmo procedimento para criação da regra acima (skype), porem altere a aplicação para **ssl** e em "Ação da Regra" escolha a opção **Somente REGISTRAR** e claro coloque uma observação descrevendo a regra. Clique no botão **Salvar**.

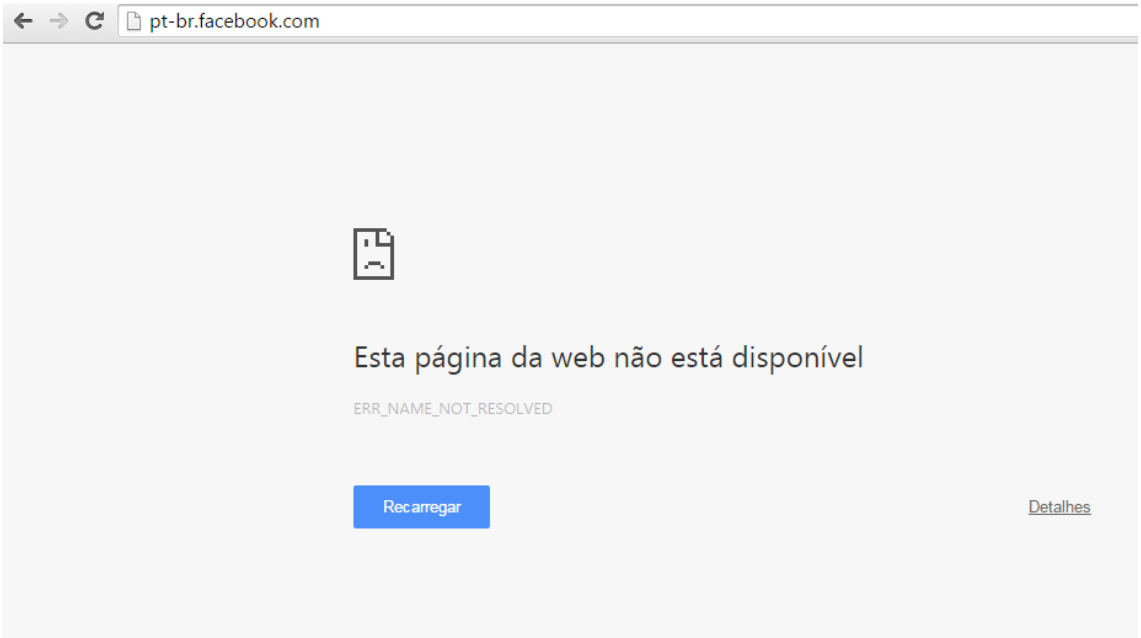


Agora que já criou a regra para registrar as aplicações SSL, podemos criar as regras para as demais aplicações, da mesma maneira que foi explicada no capítulo 3.

IMPORTANTE: esta regra de registro de aplicações SSL deve ficar sempre acima das aplicações que utilizam a criptografia SSL, conforme a figura abaixo.



Tentativa de se conectar ao Facebook depois que as regras foram criadas.



5. Para saber mais

http://www.netdeep.com.br/firewall