Centro Universitário do Rio Grande do Norte – UNI-RN
Bacharelado em Sistemas de Informação

Sistema de Detecção de Intrusão (IDS) com Snort e pfSense

- **Componentes:**
  - Alexandro Marcos Nasario do Nascimento
  - Osvaldo Soares Júnior
  - Zacarias Monteiro Honório
- **Orientador:**
  - Gilles Veleneuve Trindade Silvano

Introdução

Atualmente existe uma grande demanda de serviços web que fazem uso de diversas aplicações, que nem sempre são consideradas seguras e, por sua vez, são alvos de ataques de hackers. E quando um sistema é inseguro, ou usa algum software que contenha alguma vulnerabilidade conhecida, alguns ataques podem ser executados de forma bastante simples.

Hoje, qualquer serviço, computador ou rede que esteja acessando a Internet poderá ser alvo de um ataque, como também qualquer computador com acesso à Internet pode participar de um ataque. Normalmente os incidentes ocorrem explorando as vulnerabilidades que são encontradas em diversos alvos, como instituições bancárias, instituições governamentais, usuários domésticos, entre outros. Nesses ataques são usadas as mais variadas técnicas, tais como, negação de serviço, phishing, worms, trojans e keyloggers. Sendo assim, tornar os serviços online seguros é imprescindivel para qualquer instituição.

Problema Analisado

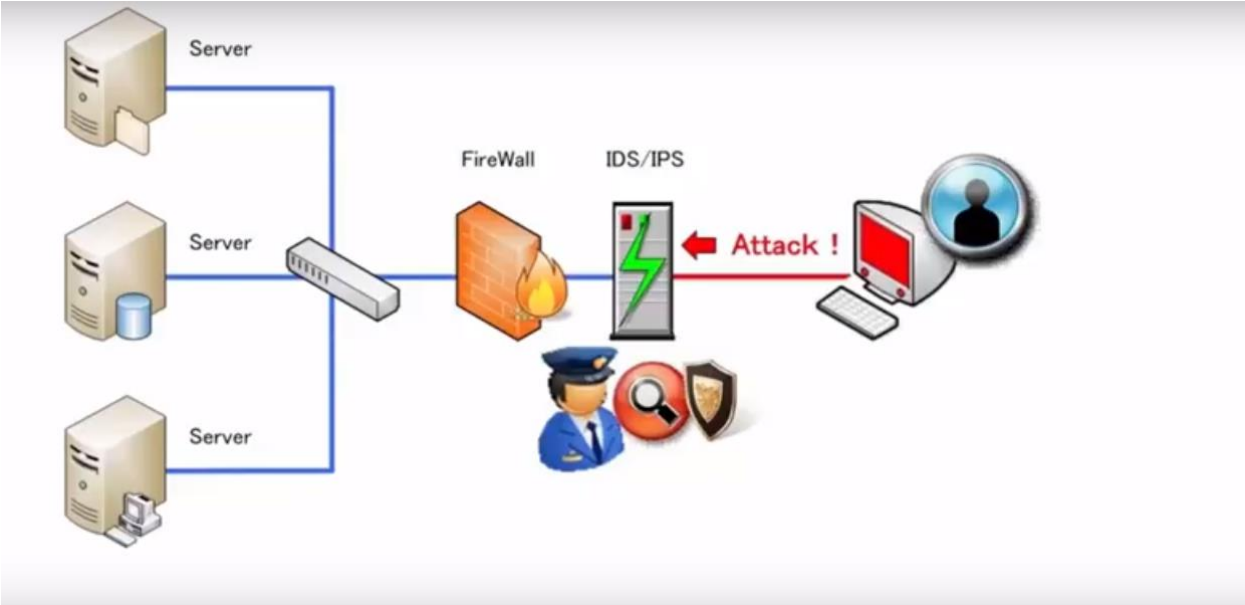
Uma instituição de ensino do porte do UNI-RN, que recebe milhares de acessos por dia, precisa ter uma proteção aprimorada contra ataques, ou seja, um ambiente que detecte e exponha em tempo real as ameaças e que aumente a capacidade para neutraliza-las de uma forma rápida e simples.

Existem diversas ferramentas que contribuem significativamente para melhoria da segurança de uma rede, tais como: a criptografia, que estabelece um nível de proteção para dados; o uso de firewalls, que estabelecem uma lógica na entrada e saída da rede controlando o tráfego a nível de pacotes; a VPN que cria um túnel criptografado entre 2 pontos de rede; entre outras.

IDS

Sendo uma ferramenta mais específica para tornar a rede mais segura, o IDS (Intrusion Detections System, no português, Sistema de Detecção de Intrusão) merece destaque especial, pois engloba o processo de monitorar, identificar e notificar a ocorrência de atividades maliciosas, não-autorizadas e que tenham como alvo os usuários de determinada rede e os coloque em risco.

Um IDS é um mecanismo que tem como principal função detectar diversos ataques e intrusões em redes de computadores, trabalhando como uma câmera ou alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas ou em desvios de comportamento.



Existem dois tipos primários de IDS, o HIDS, que é baseado em Host e monitora e analisa informações coletadas de um único host (máquina) e o NIDS, que é baseado em Rede e monitora e analisa todo o tráfego no segmento da rede. O aprimoramento das tecnologias levou ao desenvolvimento do IDS híbrido, o chamado Hybrid IDS, que utiliza as características dos dois.

E qual IDS Implementar?

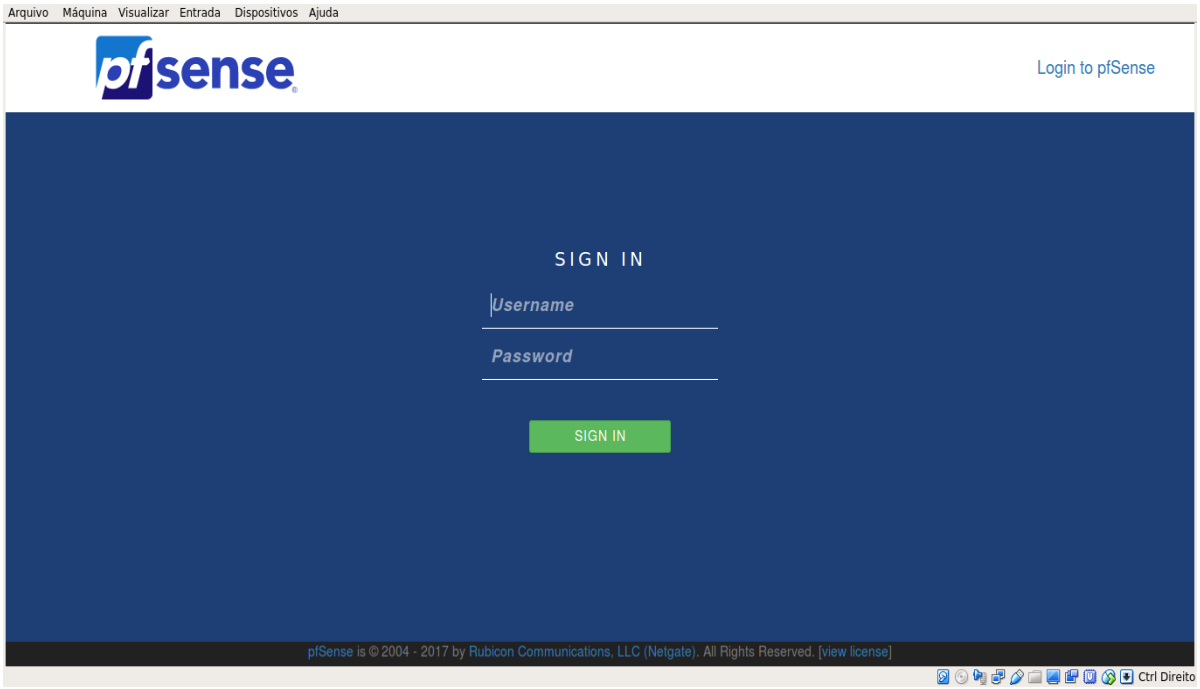
Fizemos uso de uma forma bastante prática e relativamente simples de implementar um IDS, utilizando o Snort, que é um IDS de código aberto e pode ser facilmente instalado em um firewall, como o pfSense. O Snort também pode ser configurado para funcionar como um sistema de prevenção de intrusão (IPS), tornando-o muito útil e flexível.

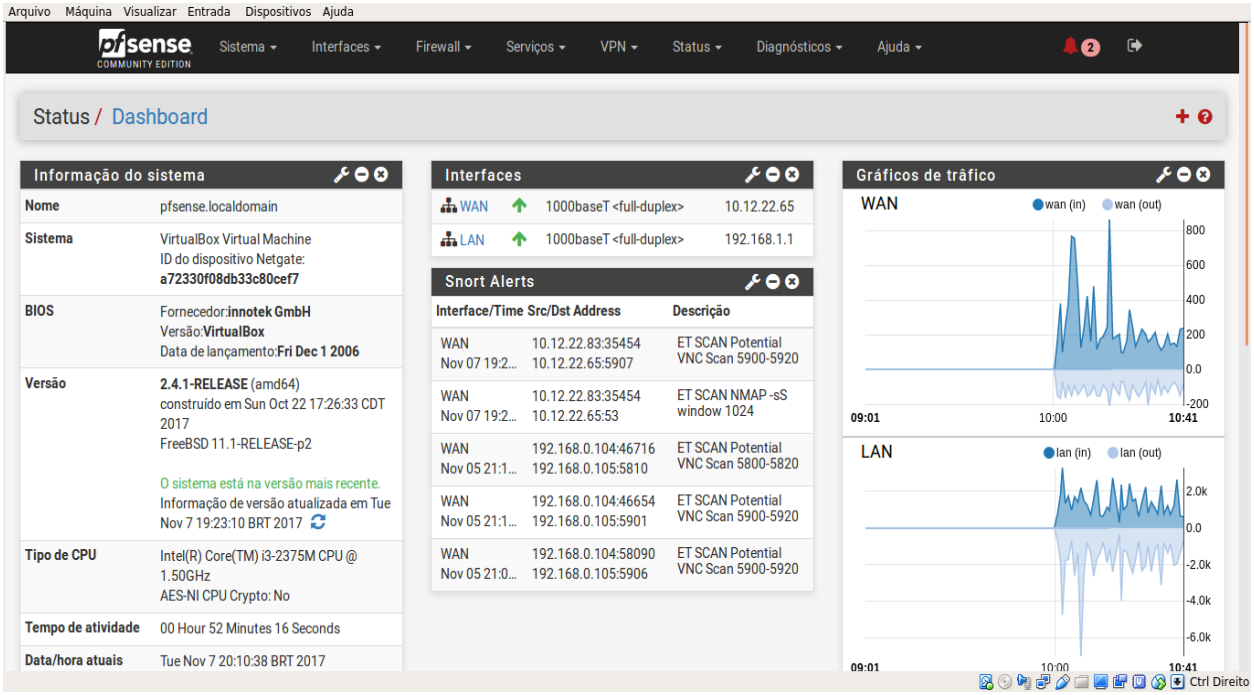
Sistema Operacional

Para o sistema operacional foi implementado o pfSense. Esse projeto é uma distribuição gratuita de firewall de rede, com base no sistema operacional FreeBSD com um kernel personalizado e incluindo pacotes de software gratuitos de terceiros para funcionalidades adicionais.

O software pfSense, com a ajuda do sistema de pacotes, é capaz de fornecer as mesmas funcionalidades (ou até mais) que as presentes em firewalls comerciais comuns, sem nenhuma limitação artificial.

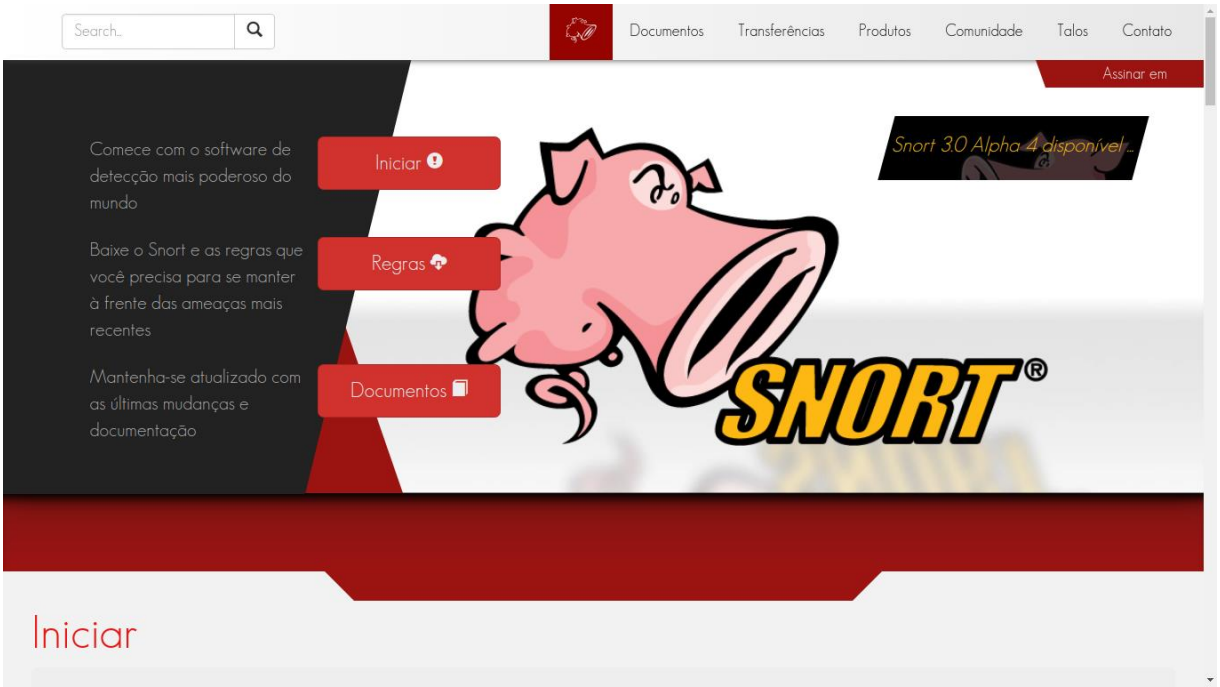
O pfSense contém uma interface web para a configuração de todos os componentes incluídos. Não é necessário possuir conhecimentos UNIX, usar linhas de comando ou editar manualmente quaisquer conjuntos de regras.





Snort

O Snort é um IDS Open Source baseado em redes, capaz de realizar análise de tráfego e captura de pacotes em tempo real em redes que utilizam o protocolo IP. Pode analisar protocolos, buscar por conteúdos específicos, e ser utilizado para detectar uma variedade de ataques e sondas.

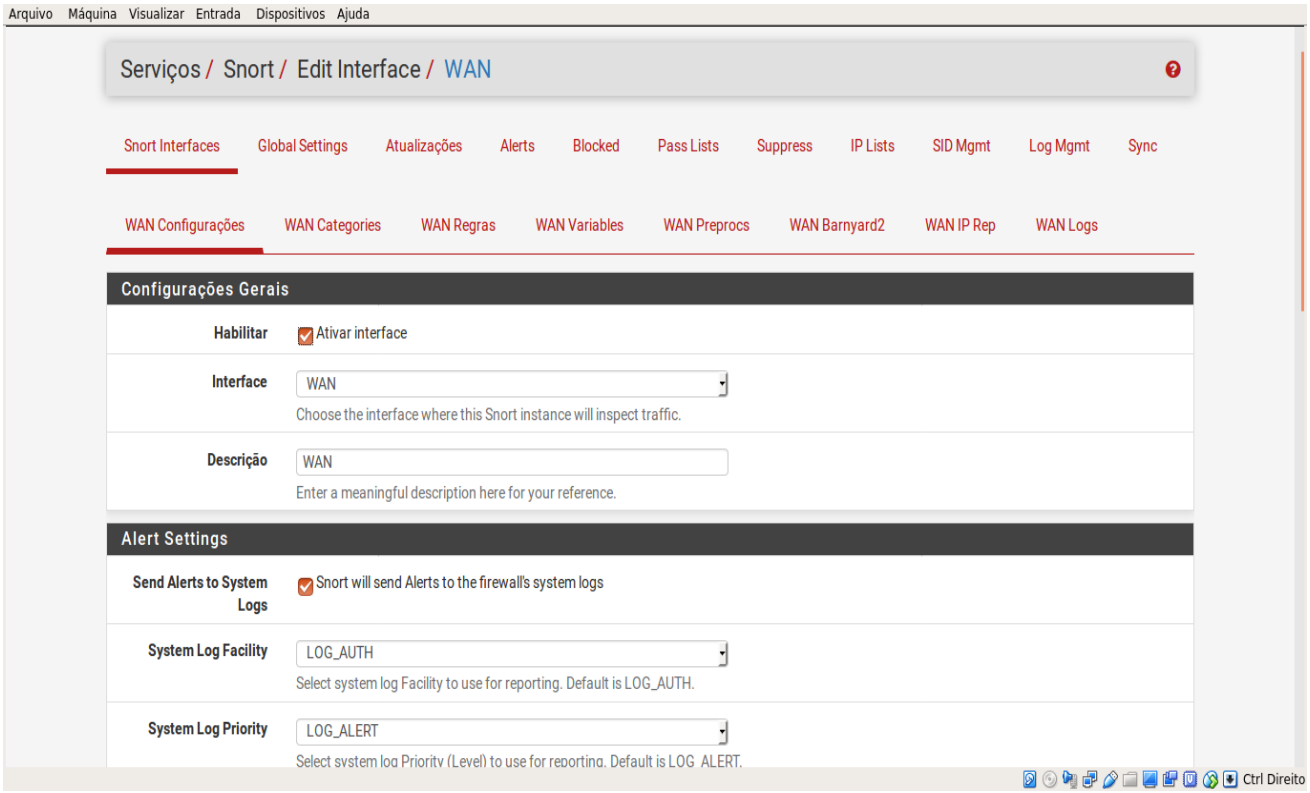


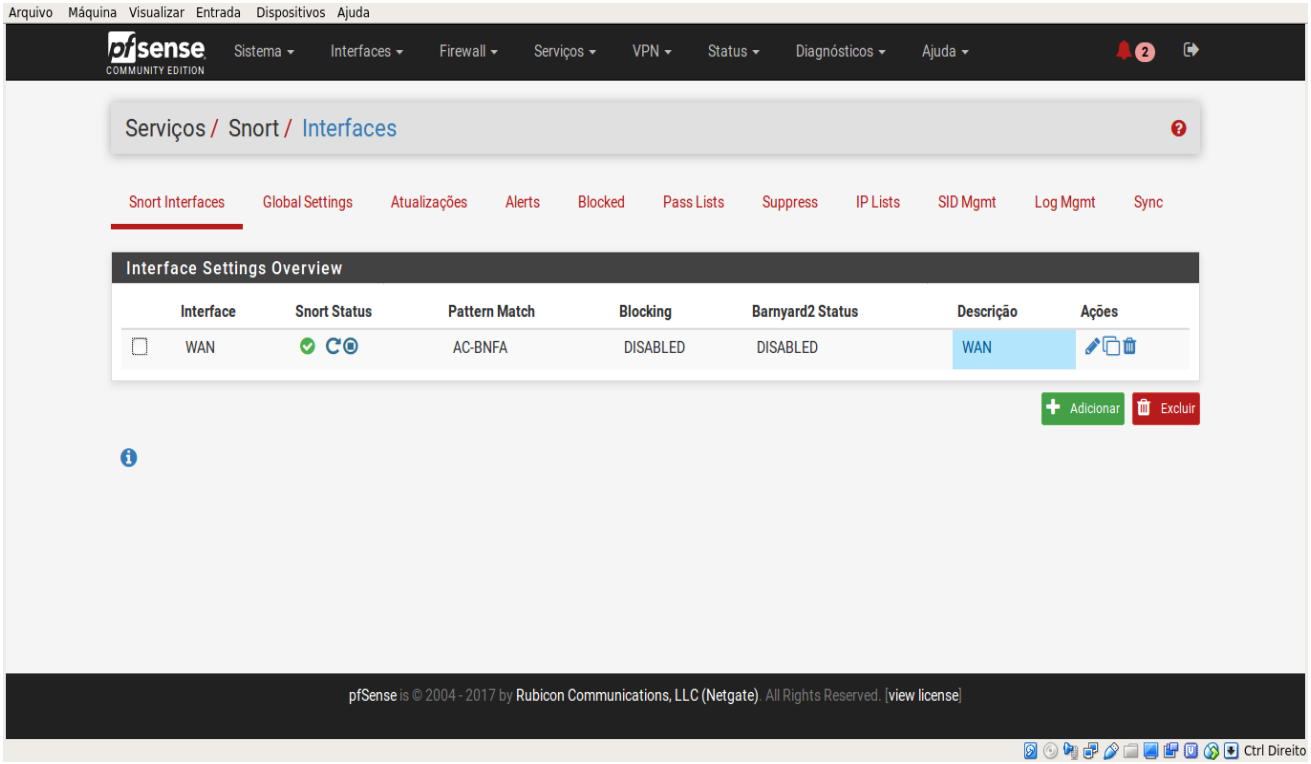
O Snort foi instalado como um pacote pfSense. Uma vez instalado, pode-se configurar uma das mais variadas instâncias do Snort para ser executar no pfSense. Cada instância é executada com configurações individuais e conta com uma interface virtual particular.

Adicionando Interfaces

Antes que o Snort possa de fato começar a funcionar como um IDS, devemos atribuir interfaces para que ele possa monitorar. Uma configuração típica é usar o Snort para monitorar todas as interfaces WAN. Outra configuração bastante comum é usar o Snort para monitorar tanto a interface WAN como a LAN.

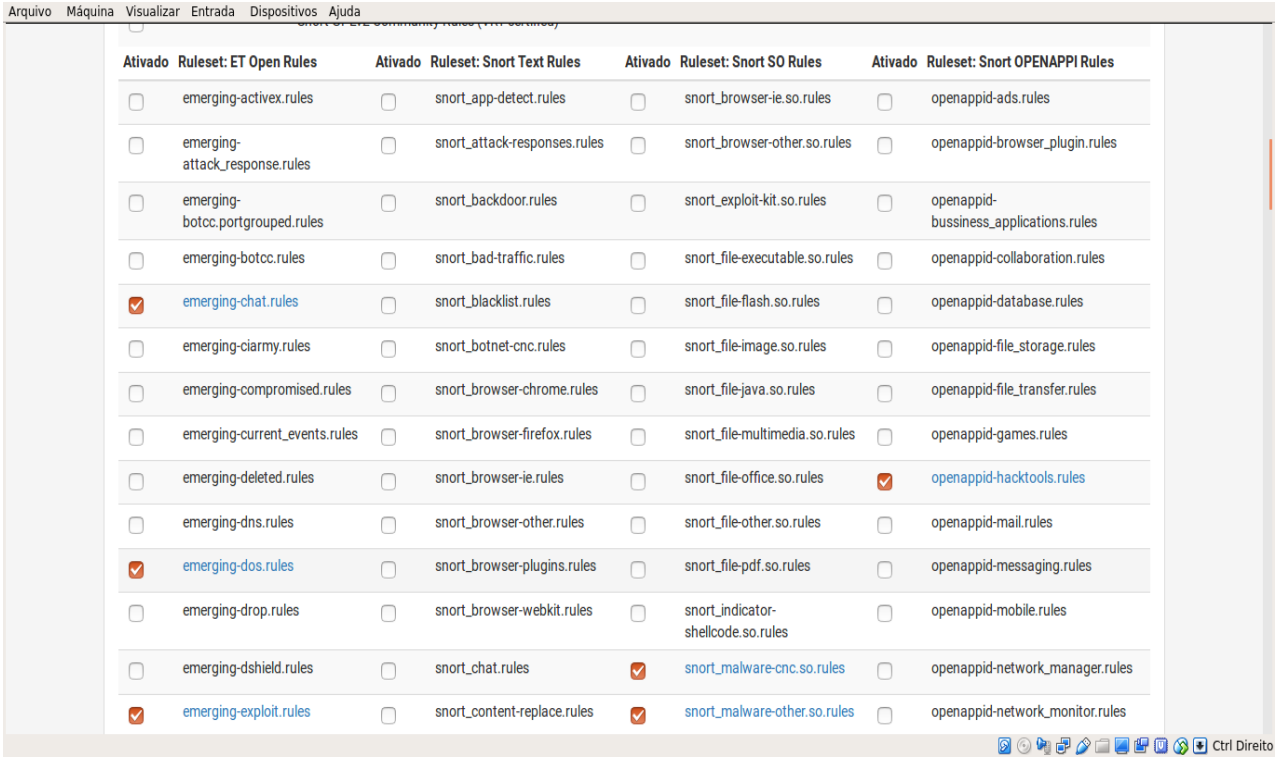
O monitoramento da interface LAN pode fornecer alguma visibilidade para os ataques em curso dentro da sua rede. Não é incomum que um PC na rede LAN fique infectado com malware e comece a lançar ataques em sistemas dentro e fora da rede.





Selecionando Categorias de Regras

O Snort faz a sua detecção baseado em assinaturas e utiliza uma linguagem flexível de regras para analisar o tráfego coletado.



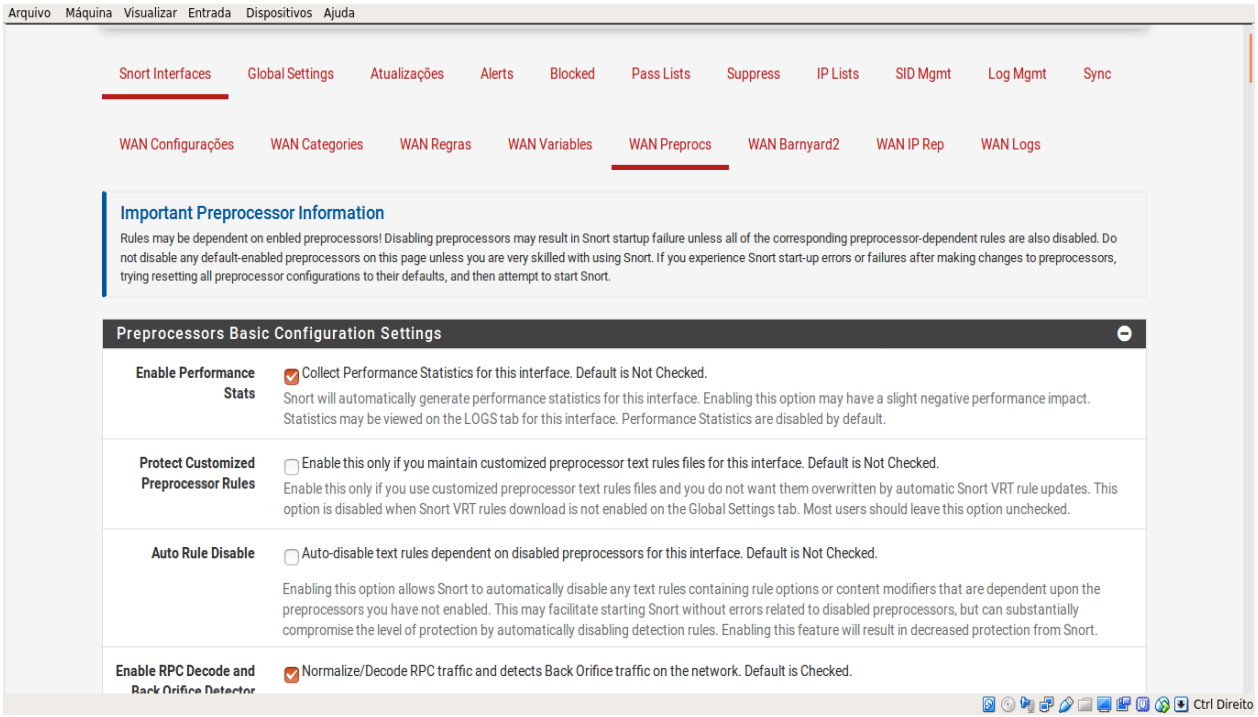
Todas as regras de detecção são divididas em categorias. E, ao dividir as regras em categorias, é possível ativar apenas as categorias específicas nas quais há interesse.

Categorias populares de regras Snort

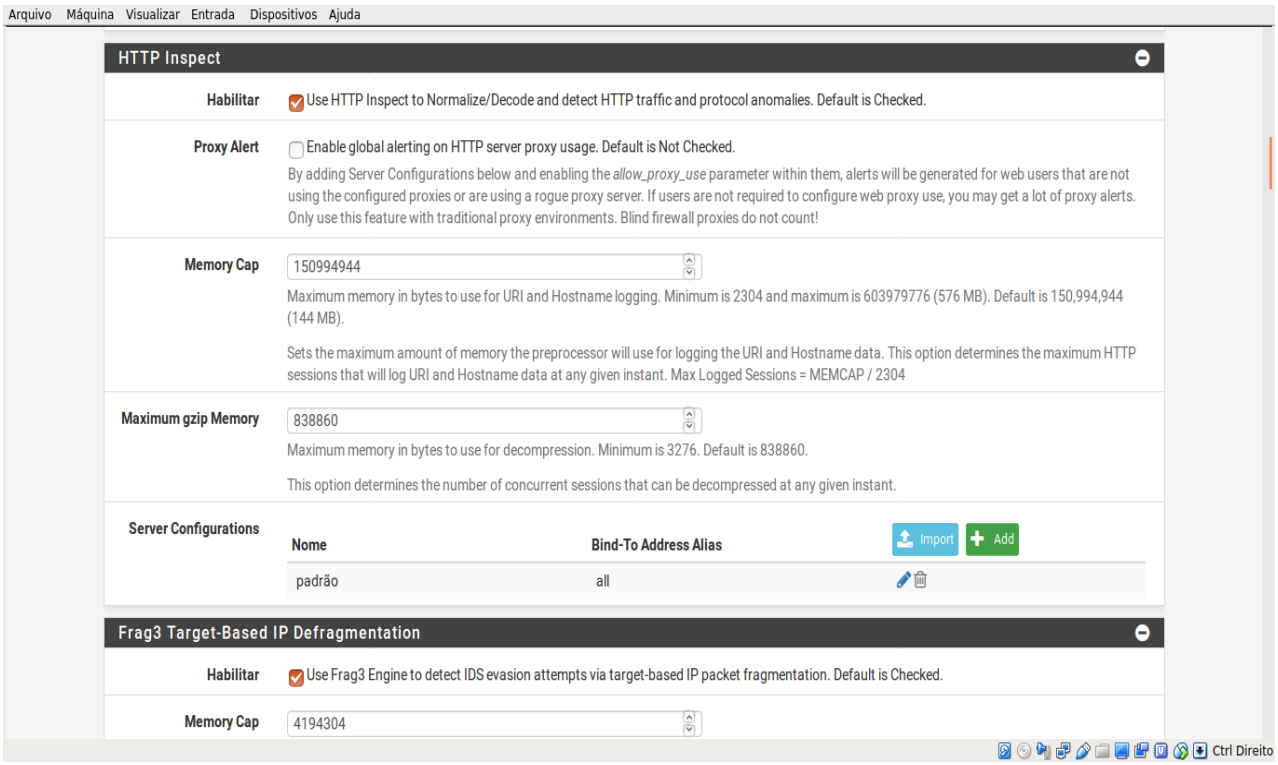
Nome da Categoria	Descrição
snort_botnet-cnc.rules	Destina conhecimentos de botnet com comando e controle de hosts.
snort_ddos.rules	Detecta ataques de negação de serviço.
snort_scan.rules	Essas regras detectam varreduras de portas, sondas Nessus e outros ataques de coleta de informações.
snort_virus.rules	Detecta assinaturas de trojans, vírus e worm conhecidos. É altamente recomendável usar esta categoria.

Pré-processadores e Configurações de Fluxo

Além de suas regras, o Snort também trabalha com os chamados "pré-processadores". Estes, por sua vez, realizam funções específicas e cruciais para a eficiência do Snort, como por exemplo, detectar portscans, detectar padrões de ataques mais complexos e mecanismos para remontar sequências de pacotes fragmentados.

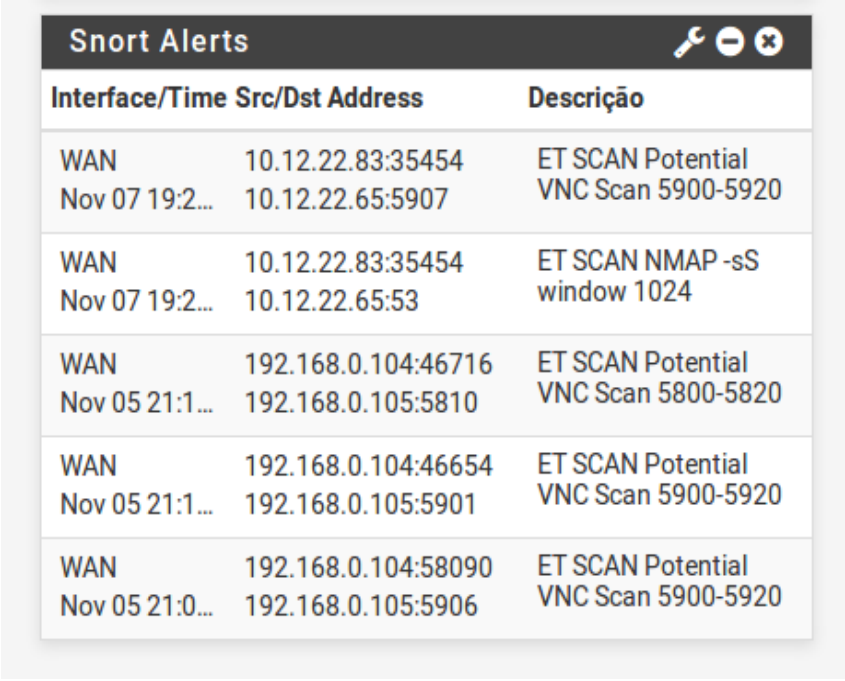


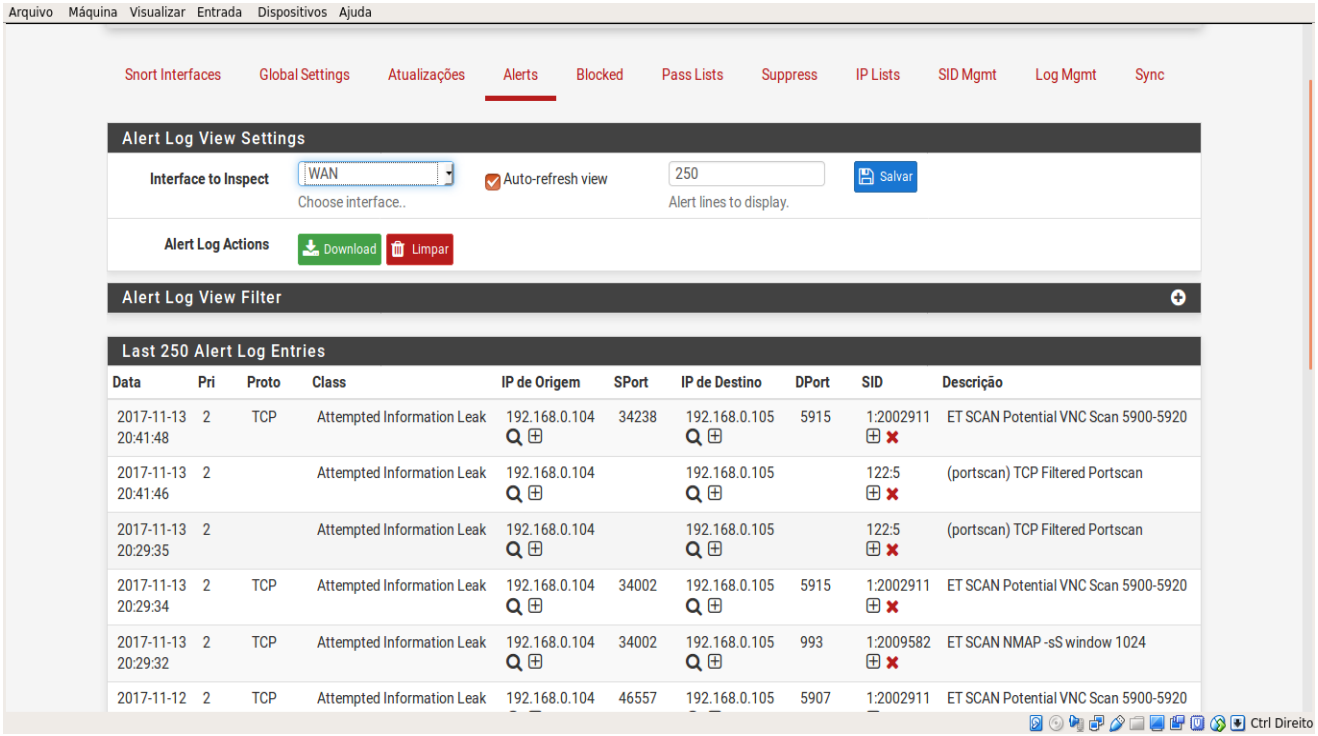
Muitas das regras de detecção requerem inspeção HTTP para serem habilitadas e para que funcionem.



Verificando Alertas

Depois que o Snort é configurado e iniciado com sucesso, devemos começar a ver alertas, uma vez que o tráfego que combina com as regras é detectado.





Os alertas gerados pelo Snort podem ser visualizados na guia **Alerts**. Se o Snort estiver sendo executando em mais de uma interface, é possível escolher a interface que exibirá os alertas.

A coluna **Data** mostra a data e o horário em que o alerta foi gerado.

A coluna **SID** contém dois ícones. O ícone + irá adicionar automaticamente o SID à lista de supressão para a interface e suprimir alertas futuros da assinatura para todos os endereços IPs. O ícone **x** na coluna **SID** desativará e removerá a regra do conjunto de regras de execução.

Na coluna **IP de Origem**, a **lupa** pode ser usada para realizar pesquisas de DNS reversas nos endereços IPs, e o ícone + pode ser usado para adicionar uma entrada de supressão automática para o alerta usando o endereço IP e SID (ID de assinatura). Isso impedirá que alertas futuros sejam gerados pela regra para esse endereço IP específico.

As demais colunas mostram dados da regra que gerou o alerta.

Conclusão

Seja para monitorar ou analisar atividades suspeitas na rede e/ou realizar auditoria na infraestrutura (de acordo com as vulnerabilidades existentes), um IDS se faz fundamental para otimizar os controles de segurança da empresa e entender melhor as tentativas e vetores de ataques que vêm surgindo ao longo do tempo. É bom frisar que a utilização de um IDS não atende à todas as necessidades de segurança de uma organização, sendo necessário utilizar outro(s) mecanismo(s) para auxiliar na proteção do perímetro. Diversas ferramentas já citadas no texto podem auxiliar na segurança das redes de uma instituição e no tráfego de informações que pode acontecer nestas.

Assim sendo, a implantação de ferramentas como essas em uma instituição como o UNI-RN não só daria maior controle ao Setor de Redes (até mesmo a TI como um todo) sobre vulnerabilidades e ataques que estão acontecendo (ou podem acontecer) nas dependências da instituição, como também traria mais segurança para os usuários que acessam as redes disponíveis, como resultado das ações preventivas tomadas pela Universidade.

Seria interessante ter ferramentas como essas na instituição, pois seria possível tomar conhecimento dos ataques que estão acontecendo e, com isso, tomar ações contra esses ataques e, assim, melhorar o aspecto da segurança das redes da Universidade, que parecem sequer ter algum mecanismo que previna ataques ou que “proteja” os usuários destes, devido à alta facilidade de se realizar ataques dentro da mesma e não sofrer absolutamente nenhuma punição ou sequer ser descoberto.

Referências

- CARLOS, Jean. **Tutorial: Instalando e configurando (IDS/IPS) Snort IDS.** Disponível em:<http://www.friendsti.com.br/tutorial-instalando-e-configurando-idsips-snortids/>Acesso em: 09 de novembro de 2017.
- **Como instalar e configurar Snort no pfSense Firewall**. Disponível em:<https://linoxide.com/firewall/install-configure-snort-pfsense-firewall/>Acesso em: 08 de novembro de 2017.
- Documentation pfSense. **Snort Alerts**. Disponível em: <https://doc.pfsense.org/index.php/Snort_alerts> Acesso em: 23 de outubro de 2017.
- **pfSense**. Disponível em: <https://www.pfsense.org> Acesso em: 23 de outubro de 2017.
- **Snort**. Disponível em: <https://snort.org/> Acesso em: 25 de outubro de 2017.