

## CHRISTIAN SIEDSCHLAG

A contribuição para este artigo ocorreu de forma igual, pois trabalhamos juntos em todo o desenvolvimento.

Para a elaboração deste artigo procuramos inicialmente dar uma visão geral do que é um sistema de prevenção e detecção de intrusos, bem como suas estratégias mais comuns de colocação e seus tipos, a fim de esclarecer o assunto para pessoas que não conheciam o conceito desta poderosa solução de segurança.

Após contextualização inicial, começamos a falar sobre a ferramenta instalada na empresa, sobre a estratégia de colocação, instalação e recursos básicos de administração. Os recursos explanados foram os mais usuais e importantes, como módulo de vacinas, auditoria, relatórios, atualizações, análise *on-line* e outros.

Por fim falamos um pouco de nossa experiência na administração, instalação e os resultados obtidos após poucos dias de funcionamento.

Esperamos que as pessoas possam ter uma visão do quão importante é a utilização de uma solução de prevenção e detecção de intrusos no ambiente corporativo.

# **Estudo da solução de prevenção e detecção de intrusos integrado (IPS/IDS)**

*Christian Siedschlag, Juliana Correa*

Curso de Especialização em Redes e Segurança de Sistemas  
Pontifícia Universidade Católica do Paraná

Curitiba, 29 de Setembro de 2009

## **Resumo**

*O objetivo deste trabalho é avaliar o funcionamento da solução de IPS/IDS integrado do fabricante IBM. Além do conceito teórico, será abordada topologia de rede ao qual a solução foi implantada, funcionamento superficial, vacinas, regras de auditoria e geração de relatórios. Será contemplado neste estudo, solução baseada em Rede e Host. Para um entendimento mais abrangente, serão comentadas algumas estratégias de deployment recomendadas pela SANS (SysAdmin, Audit, Network, Security).*

## **1 Introdução**

Os sistemas informatizados atuais em comparação com poucos anos atrás estão muito avançados. A sociedade tem confiado cada vez mais nos ambientes computacionais que variam entre simples redes caseiras, conectadas geralmente á rápidas ADSL's, à redes empresariais maiores, interligadas ao redor do mundo. O agendamento de um taxi, compras on-line, banco on-line ou mesmo a leitura de notícias na internet são convenientes. Esta grande confiança e conveniência, acoplada ao fato de que os ataques estão se tornando cada vez mais freqüentes, têm aumentado a necessidade de controles de segurança a fim de minimizar os riscos.

Tal risco está sendo ignorado por muitas pessoas ao qual utilizam sistemas on-line em suas casas ou em pequenos escritórios. Há casos em que o risco não é completamente ignorado e os donos dos sistemas instalam firewalls para proteger seus servidores web ou servidores de e-mail para sentirem-se mais seguros. A condução de negócios sobre www (*world wide web*) ou comunicação sobre sistemas de e-mail tem sido alvo de ataques automatizados. Muitos firewalls controlam acesso somente bloqueado endereços ips ou portas. Se o usuário possui um sistema de e-mail e deseja comunicar-se com sistemas

externos, deveria abrir a porta 25 para o mundo externo. Mas o que acontece quando um ataque ocorre sobre a porta 25? Sem possuir algum sistema que analise pacotes, o servidor de e-mail estará à mercê de ataques [1].

## 2 O que é IDS e IPS

Os IDS's (*Intrusion Detection Systems*) são sistemas de coleta e análise de informações que permitem a automatização do processo de identificação de incidentes de segurança. Estes sistemas trabalham, basicamente, coletando informações em diferentes pontos de uma rede, inclusive dentro de *hosts* e analisam estas informações em busca de padrões de comportamento que caracterizem ataques. Devido, ao grande número de acessos que a maioria das redes possui, é impossível fazer este trabalho de forma manual. Sendo assim, o IDS é uma ferramenta de monitoramento fundamental para a segurança em redes e sistemas [2].

Já o termo IPS pode ser associado a um sistema, *hardware* ou *software*, capaz de reagir às mudanças da rede. Estes conseguem encontrar focos de intrusão, conhecidos ou não, e agir sobre eles prevenindo a intrusão de ser bem sucedida [3].

Com o passar dos tempos, as funcionalidades de monitoramento começaram a ser movidas para dentro de dispositivos de controle de acesso. Desta forma, ao invés de detectar ataques analisando informações que foram geradas posteriormente ao acontecimento dos incidentes, as mesmas tecnologias podem ser utilizadas antes de se tomar a decisão de permitir ou não acesso a um pacote. Este tipo de tecnologia vem sendo incorporada em *firewalls* para criar produtos híbridos que combinam ambas as tecnologias, chamados de IPS (*Intrusion Prevention Systems*) [2].

Sistemas de Detecção e Intrusão podem ser classificados quanto à localização deste na rede. Existem dois grandes tipos: baseado em máquina (*host*) e baseado em rede.

### 2.1 IPS/IDS Máquina (*host*)

IPS baseado em máquina é uma extensão do IDS baseado em máquina, o qual monitora eventos da máquina varrendo pelos recursos em atividade. Estes reportam qualquer evento que é descoberto em bases de dados seguras e verificam se o evento reportado está relacionado a eventos maliciosos contidos em bases de conhecimentos já conhecidas [4]. No caso do IPS, há uma ação que é tomada conforme o evento reconhecido.

Os IDS's baseados em *host* coletam informações dentro das máquinas monitoradas, o que, normalmente, é feito através de um *software* instalado dentro delas, ao qual devem ser bastante leve e suportado por todas as plataformas. Os IPS/IDS possuem muitas vantagens: são capazes de monitorar e bloquear ataques mesmo em caso de comunicação codificada e tem uma grande visibilidade sobre o que acontece dentro da máquina. Algumas soluções podem até reagir prontamente a problemas, restaurando, por exemplo, a página original de um site que tenha sofrido pichação ou recuperando um arquivo de sistema comprometido [2].

### 2.2 IPS/IDS Rede

IPS's baseados em rede são componentes que se encontram dentro da rede, e procuram por ataques [4]. O diferencial deste tipo de IPS, é que este faz o isolamento de tráfego, ou seja, consegue caracterizar e bloquear o tráfego suspeito [3].

Neste tipo de sistema, as informações são coletadas na rede, normalmente através de dispositivos dedicados que funcionam de maneira muito similar a *sniffers* de pacotes. Portanto, o dispositivo possui uma interface de rede atuando de forma promíscua, ao qual ele está conectado. A principal vantagem de IPS/IDS baseados em rede é o fato de que diversas máquinas podem ser protegidas utilizando-se apenas um agente. Obviamente, o fator desempenho acaba sendo o limitador de quantos pacotes a solução é capaz de analisar [2].

### 3 Topologia – Posicionamentos padrões

Uma vez avaliados todos os requisitos básicos e necessidades a serem endereçadas pela solução de IPS/IDS, a implementação pode efetivamente começar. Neste momento, as dúvidas mais comuns podem estar relacionadas à colocação dos componentes.

Os agentes baseados em máquina (*host*) não deixam dúvida sobre o local de instalação, já que devem estar dentro das máquinas que serão monitoradas por eles. Porém, deve-se analisar se haverá conectividade entre eles e o local que foi escolhido para a colocação do gerenciador. O volume de informações geradas pelos agentes tende ser grande e convém também considerar o consumo dos *links* caso o gerenciador esteja em uma localidade remota [2].

O componente que geralmente traz mais dúvida em relação à colocação é o agente de rede, pois, dependendo do local, pode-se dar um foco completamente diferente no funcionamento do dispositivo. A seguir uma lista com as opções de posicionamento mais comuns [2]:

- À frente do *firewall*: Neste local, o agente tem a capacidade de monitorar ou bloquear todo o tráfego que entra e sai da rede. Normalmente, através de filtros, apenas o tráfego tendo como destino o firewall e a DMZ são selecionados. Aqui o agente terá uma capacidade limitada de ataques que surjam a partir da rede interna.
- Na rede interna: Esta colocação serve, basicamente, para monitorar/bloquear ataques aos servidores internos, especialmente os que partem de máquinas da própria rede interna. Logo após a proteção dos servidores da DMZ, este seria o próximo agente a ser colocado.
- Na DMZ: A DMZ é o segmento de rede que mais necessita de um agente de IPS/IDS. Os servidores estão altamente expostos e o próprio conceito de DMZ prevê que haja a capacidade de detectar e reagir a ataques antes que eles atinjam a rede interna. Além disso, o tráfego que alcança este segmento já cruzou o *firewall*, ou seja, a primeira camada que protege os equipamentos que se encontram na DMZ.

### 4 Topologia – Posicionamento adotado para implantação na empresa

A estratégia adotada para implantação da solução de IPS/IDS de rede foi à frente do firewall. Foi a que melhor adequou-se ao ambiente corporativo, pois todo o tráfego estará sendo inspecionado (detectando ou prevenindo) pela solução se estiverem dentro das seguintes condições:

- Tráfego saindo do segmento LAN, para a WAN ou DMZ
- Tráfego saindo do segmento DMZ, para a LAN ou WAN
- Tráfego entrante da WAN, para o segmento DMZ ou LAN

Já os IPS/IDS de host foram instalados em máquinas consideradas críticas para a empresa, por suportarem serviços de grande importância para a continuidade dos negócios, tais como: servidor de DNS, Oracle Application Server (ao qual hospeda aplicações Java acessadas internamente e externamente), Proxy Server (Squid com Squid Guard), e-Procurement

(solução utilizada por fornecedores para cotações *on-line* de suprimentos) e *Oracle Collaboration Suíte* (ao qual utiliza um banco de dados Oracle para autenticação dos usuários de e-mail e Portal).

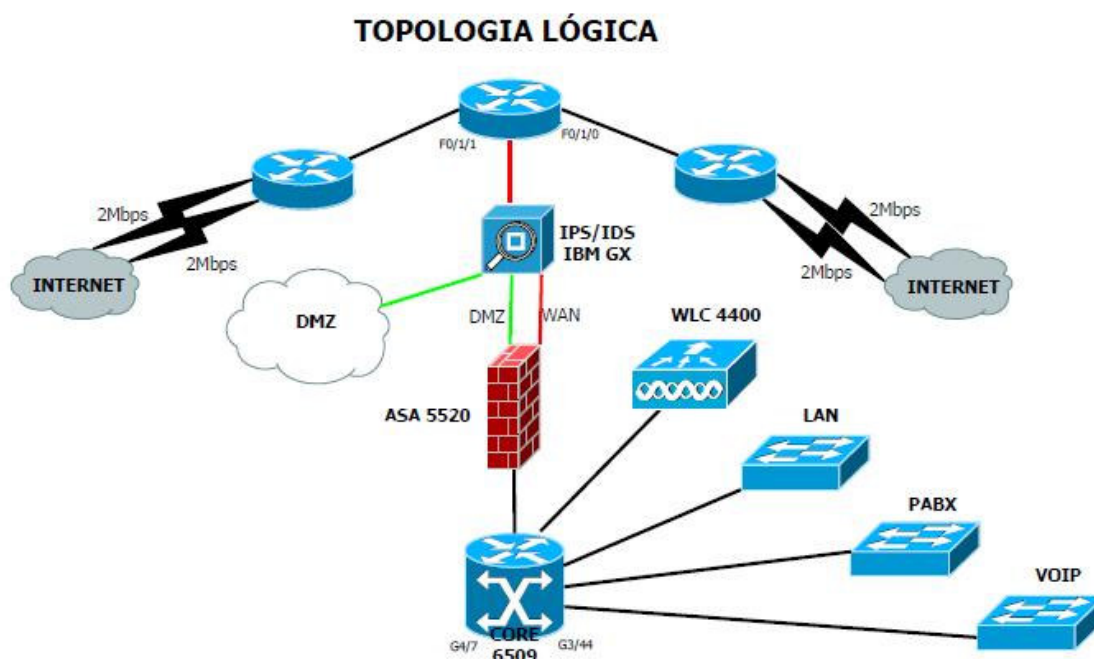


Figura 1 – Topologia de rede após implantação da solução de IPS/IDS

## 5 A solução e seus recursos (*features*) básicos de administração

A solução denominada GX 4004, foi desenvolvida pela empresa IBM com o intuito de tornar-se mais um importante aliado para as empresas, onde ajuda a detectar e bloquear os ataques antes que afetem seus negócios. Com 200 Mbps de *throughput* através de dois segmentos de rede, entrega segurança, desempenho e confiabilidade em uma solução simples para instalação e gerenciamento [5].

O dispositivo pode funcionar de três diferentes formas [6]:

- *Inline protection* – O modo *Inline Protection* permite habilitar a solução para fazer o bloqueio (prevenção) dos pacotes trafegados com base nas vacinas disponíveis.
- *Inline simulation* – O modo *Inline simulation* permite habilitar a solução para monitorar todo o tráfego de rede, sem afetar o mesmo. Utilizado geralmente no início da implantação para entender qual vacina poderia ou não ser habilitada em modo bloqueio.
- *Passive monitoring* – O modo *Passive monitoring* parece-se muito com a funcionalidade de detecção de intrusão (IDS), monitorando todo o tráfego de rede sem o equipamento estar em linha. Se o *appliance* encontra uma atividade de rede suspeita, envia um sinal de bloqueio para o pacote TCP. É muito utilizado para descobrir qual tipo de proteção *inline* sua rede necessita.

Adapter Name	Mode (Non HA)	Port ID
Card1	InlineProtection	A
Card2	InlineProtection	C
	InlineSimulation	
	Monitoring	

Figura 2 – Formas de funcionamento

Para um gerenciamento mais completo, a fim de utilizar todos os recursos necessários para administração da solução, é necessário a instalação de uma console de gerenciamento chamada *SiteProtector*, ao qual é instalado com outro software de banco de dados (*SqlServer*) para armazenamento das configurações, dados de coleta e eventos. Com o *SiteProtector* pode-se gerenciar componentes, monitorar eventos e agendar relatórios. Esta console de gerenciamento é composta por vários recursos. Podemos citar alguns deles abaixo:

- **Agent Manager** – Fornece as seguintes funções para componentes e agentes do sistema:
  - Gerencia comandos e atividades de controle
  - Facilita a transferência de dados para o coletor de eventos
  - Controla atualizações de vacinas, bancos de dados, coletor de eventos e atualização de firmware [7]

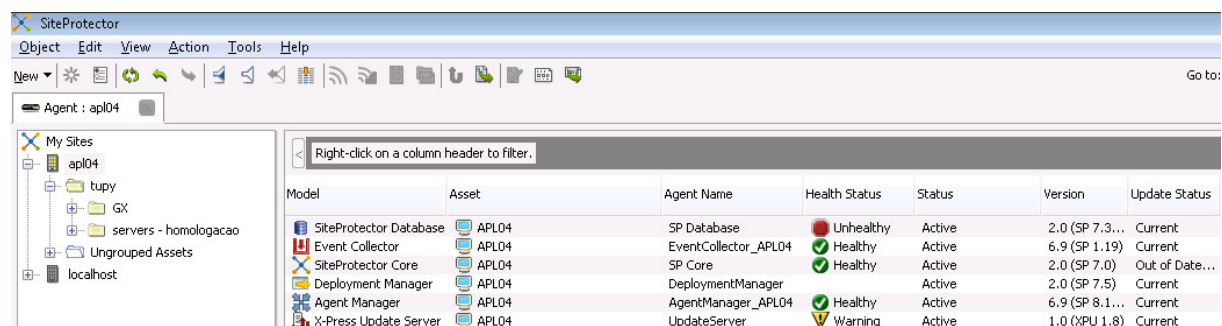


Figura 3 – Tela do *Agent Manager*

- **Analysis** – Recurso utilizado para visualizar incidentes ocorridos em tempo real ou em um determinado período. Através dele é possível detalhar o ataque, quantidade de tentativas, qual foi a origem, destino, porta, protocolo e severidade.

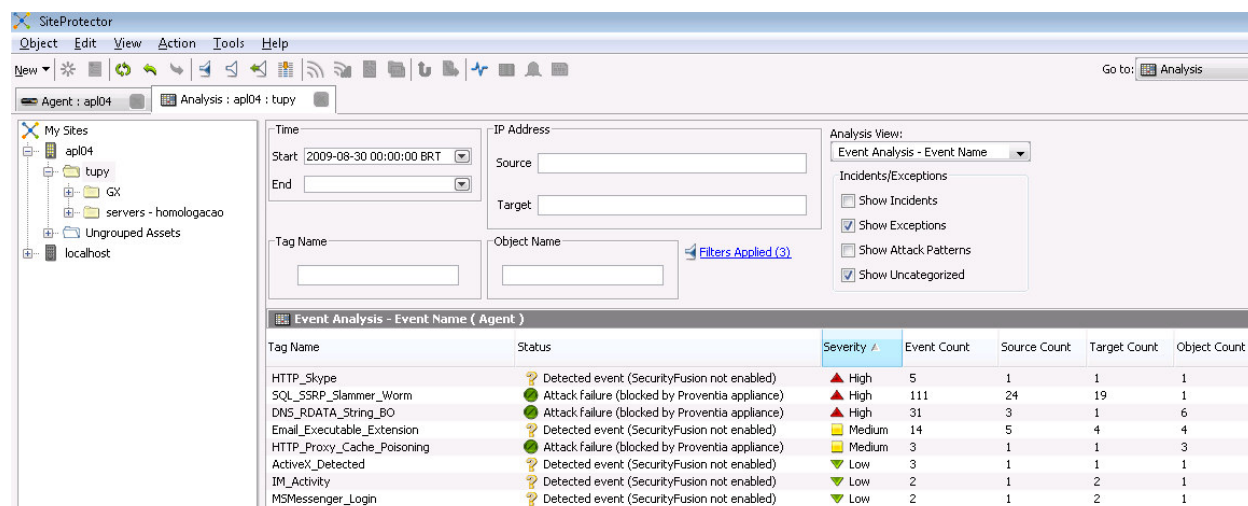


Figura 4 – Tela da opção *Analysis*

- **Asset** – São considerados *assets* os servidores individuais (IPS/IDS de host) ou um dispositivo em uma rede, neste caso a própria solução de IPS/IDS de rede. A solução do *SiteProtector* organiza os *assets* em grupos ou subgrupos para que sejam aplicadas as regras globais ou individuais de assinaturas ou auditoria [7].

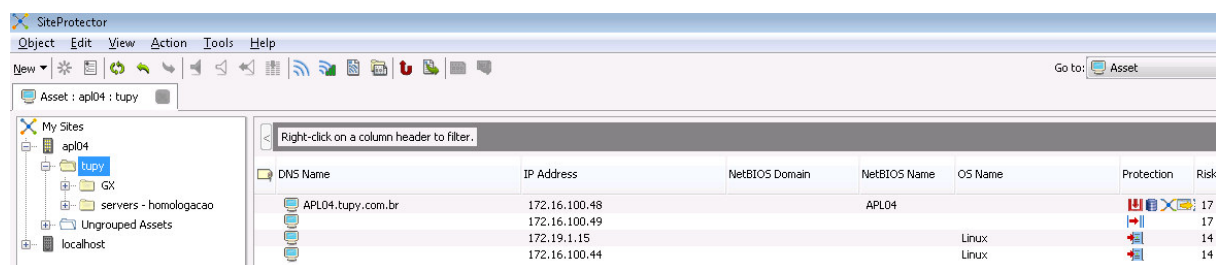


Figura 5 – Tela da opção Asset

- **Policy** – Através do recurso *Policy* são configurados as políticas de bloqueio ou detecção de intrusos através das vacinas disponíveis, bem como políticas de auditoria para os *hosts* individuais, grupos ou subgrupos.

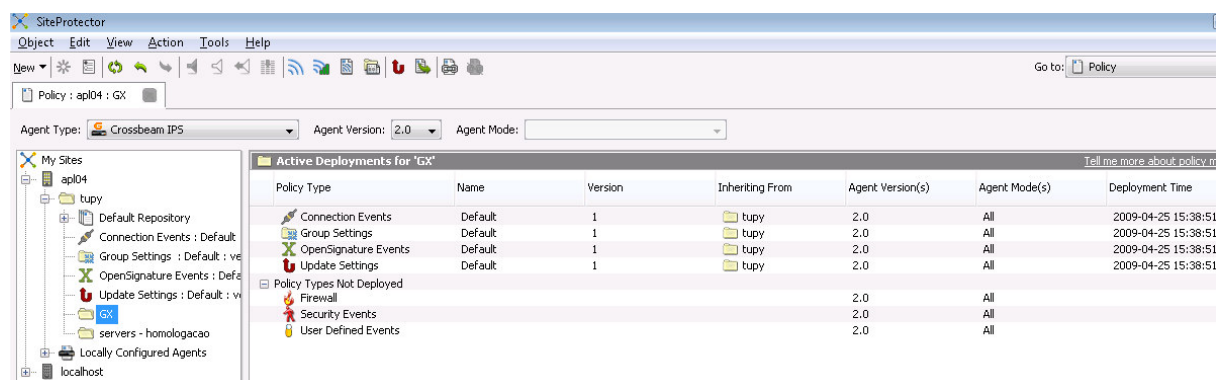


Figura 6 – Tela da opção Policy

- **Report** – Ferramenta utilizada para criar relatórios *on-line* ou agendar relatórios diários, semanais ou mensais.

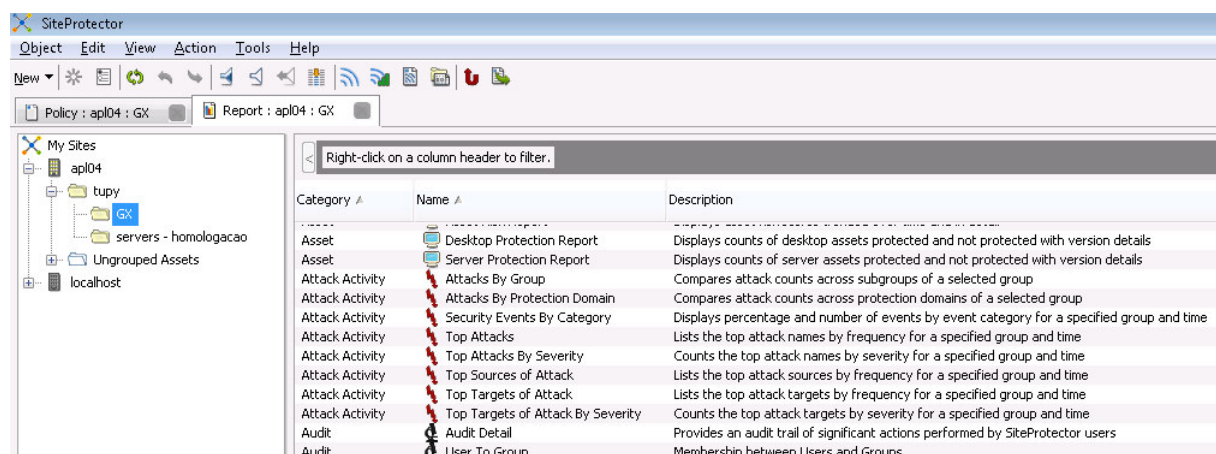


Figura 7 – Tela da opção Report

- **Summary** – Utilizado para mostrar de forma resumida informações referentes a eventos críticos, atualizações disponíveis, gráficos de ataques recentes e outros, podendo ser customizado conforme desejo.

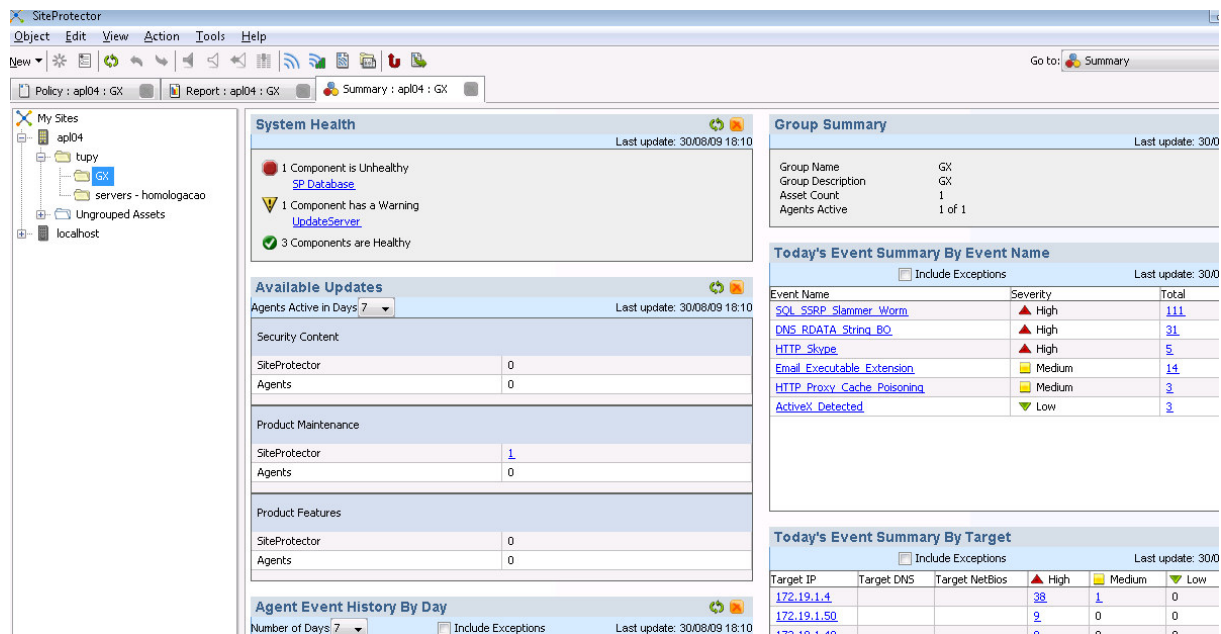


Figura 8 – Tela da opção Summary

## 6 Vacinas contra ataques

Atualmente a solução conta com mais de 2.500 vacinas, atualizadas periodicamente. Sempre que uma nova técnica de ataque é descoberta, a equipe da IBM ISS (*Internet Security Systems*) trabalha para criar uma vacina e atualizar seus clientes. Com base em cada vacina disponível, é possível configurar a solução para fazer o bloqueio ou apenas a detecção dos pacotes. Conforme ilustração abaixo, se a vacina estiver habilitada, sem estar selecionada a opção *block*, fará apenas a detecção. Se estiver habilitada e selecionada a opção *block*, será feito o bloqueio do pacote.


	Enabled	Tag Name	Severity	Protocol	Ignore Events	Display	Block
Protection Domain: Global (2 items)							
Attack/Audit: Attack (2538 items)							
	<input checked="" type="checkbox"/>	Ace_Filename_Overflow	High	ace	<input type="checkbox"/>	Witho...	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	ACF_Mem_Corruption	High	acf	<input type="checkbox"/>	Witho...	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	ActiveX_Blocked	High	html	<input type="checkbox"/>	Witho...	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	ActiveX_Warning	Low	html	<input checked="" type="checkbox"/>	Witho...	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	ATX_Pdnd_Overflow	High	tcp	<input type="checkbox"/>	Witho...	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	Allaire_JRun_JSP_Execute	High	url	<input type="checkbox"/>	Witho...	<input checked="" type="checkbox"/>

Figura 9 – Parte da tela de vacinas

Podemos citar algumas vacinas como sendo *SQL\_slammer*, *DNS\_rdata\_overflow* e *HTTP\_proxy\_cache\_poisoning*. Abaixo seguem informações sobre algumas delas como nome, descrição, sistemas afetados e como se proteger contra incidentes.


Risco	Vacina	Descrição	Sistemas Afetados	Como Remover
Alto	<i>SQL_SSRP_Slammer_Worm</i>	Este evento procura por um excesso (transbordamento) em um pacote UDP com porta de destino 1434 e o endereço de retorno do SQL	Microsoft Windows NT: 4.0, Microsoft Windows 2000, Microsoft SQL Server: 2000, Microsoft Data Engine: 2000, Cisco Unity Server: 3.0, Cisco Building Broadband Service	Administradores devem aplicar o ultimo (mais recente) patch SQL Server, como listado em Microsoft Security Bulletin MS03-031, e



		Slammer Worm. O parâmetro de sintonização do pam udp slammer drop (verdadeiro) derruba o pacote sem processamento futuro (detalhado)	Manager: 5.1, VERITAS ExecView: 3.1, VERITAS Backup Exec: 9.0, Cisco Unified CallManager: 3.3, Cisco Building Broadband Service Manager: 5.0, Cisco Unity Server: 4.0	reiniciar o sistema para proteger-se contra futuras infecções.
	<i>DNS_RDATA_TXT_overflow</i>	Esta assinatura procura por um registro de fonte malformed TXT, HINFO, X25, or ISDN com um mais longo string do que o registro de comprimento do campo, o qual pode sobrecarregar um buffer ou executar um código arbitrário. Versões mais antigas de Sendmail's LibSPF2 são vulneráveis a esta exploração.	Gentoo Linux, Debian Debian Linux: 4.0, libspf2 libspf2: 1.2.7, libspf2 libspf2: 1.2.6, libspf2 libspf2: 1.2.5, libspf2 libspf2: 1.2.4, libspf2 libspf2: 1.2.3, libspf2 libspf2: 1.2.2, libspf2 libspf2: 1.2.1, BlueCat Networks Meridius Email Gateway	Atualize para a versão mais recente do libspf2 (1.2.8 ou posterior), disponível no site da libspf2.
	<i>DNS_RDATA_String_BO</i>	Esta assinatura detecta tentativas de transbordar alguns clientes dns usando manipulações específicas de RDATA character string lengths.	Microsoft Windows 2000: SP4	Aplique o patch apropriado para seu sistema, enumeradas no Microsoft Security Bulletin MS06-041. Ver Referências.
 Medio	<i>HTTP_Proxy_Cache_Poisoning</i>	Esta assinatura detecta respostas do servidor HTTP que pode corromper os caches de servidores proxy HTTP.	Microsoft Small Business Server: 2000, Microsoft ISA Server: 2000 SP2, Microsoft Small Business Server: 2003 Premium	Aplique o patch apropriado para seu sistema, enumeradas no Microsoft Security Bulletin MS05-034.
	<i>Cross_Site_Scripting</i>	Essa assinatura é desencadeada quando bem conhecidas formas de "tag <SCRIPT>" são detectadas em dados de URL ou CGI. Esta assinatura substitui HTTP_GETargetscript, HTTP_POST_Script e eventos HTTP_Cross_Site_Scripting.	IETF HTTP/1.1	Esta verificação é apenas para fins informativos.  Garantir que o seu firewall pessoal, o sistema operacional e aplicativos são up-to-date, a fim de minimizar a ameaça de um comprometimento do sistema.

## 7 Vacinas de auditoria

A solução dispõe de mais de 400 vacinas de auditoria, ou seja, pacotes que não são considerados perigosos, mas que ajudam a proteger ainda mais as empresas. Podemos citar alguns deles como sendo proteção/detecção contra uso de *Instant Messenger*, possibilidade de gravar conversas, *streaming* de voz, P2P, *skype* e outros. Abaixo detalhamos algumas destas vacinas:

Risco	Auditoria	Descrição	Sistemas Afetados	Como Remover
 Baixo	<i>BitTorrent DHT peer-to-peer ping detected</i>	Esta assinatura via detecta Trackerless tráfego ping DHT, o que pode indicar que um peer BitTorrent / nó está presente e ativo em sua rede	BitTorrent	Esta auditoria é apenas para fins informativos.
	<i>Microsoft MSN Messenger video request detected</i>	Esta assinatura relata a inicialização de uma conferência de vídeo MSN	Microsoft Windows 2000: SP4, Microsoft Windows	

		Messenger.	2003 Server: x64, Microsoft Windows XP: SP2, Microsoft MSN Messenger: 6.2, Microsoft Windows 2003 Server: SP1, Microsoft Windows XP: Professional x64, Microsoft Windows Live Messenger: 8.0, Microsoft Windows Vista, Microsoft Windows 2003 Server	
	<i>Skype installed</i>	Esta assinatura olha para o mecanismo de atualização do Skype, que indica a presença do pedido.	Skype	Se este pedido não é permitido em sua organização, o Skype deve ser desinstalado.
⚠ Medio	<i>An email attachment sent with yahoo.com mail service</i>	Esta assinatura detecta um anexo enviado com o mail do Yahoo. Esta assinatura informa o número de anexos, os dados anexo e do destinatário do e-mail.	Diversos fabricantes e qualquer aplicação	Verifique todos os anexos para garantir que não haja .Exe ou .GVI ou qualquer outra coisa suspeita.

## 8 Relatórios

A ferramenta *SiteProtector* possui em torno de sessenta relatórios divididos em categorias para serem utilizadas de forma *on-line* ou através de agendamento. Tais categorias dividem-se em Ataques, Auditoria, Filtro de e-mail, Vírus e outros. Selecionamos alguns relatórios a fim de obtermos um entendimento mais detalhado.

- ***Attacks by Protection Domain***

Neste relatório podemos observar a quantidade total de ataques em um período pré-definido por nível de risco: baixo, médio e alto.

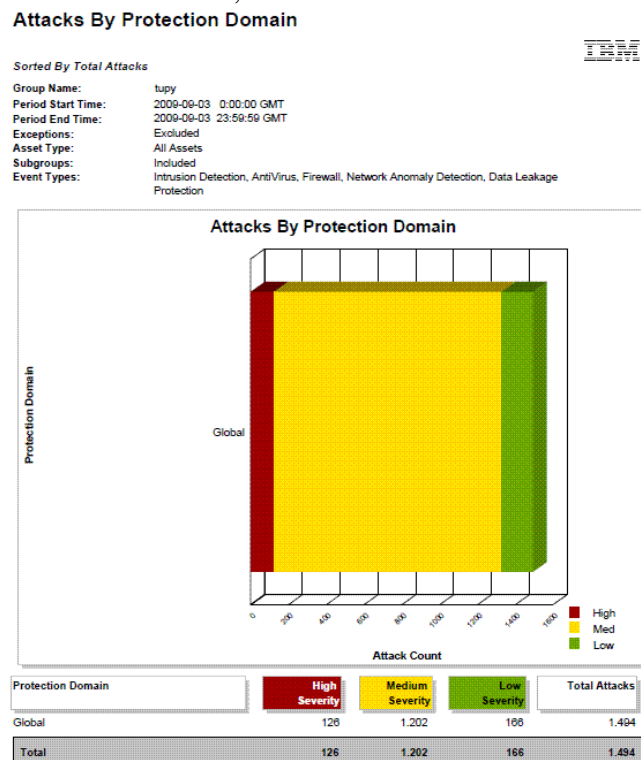


Figura 10 – Relatório de ataques em um período

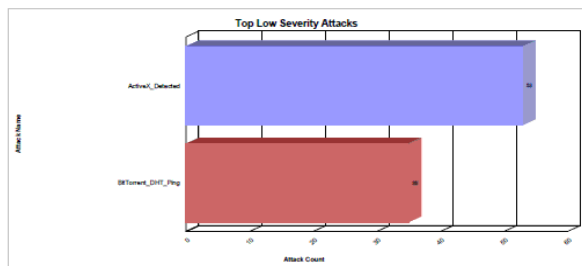
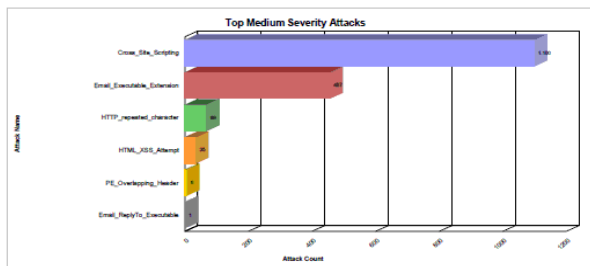
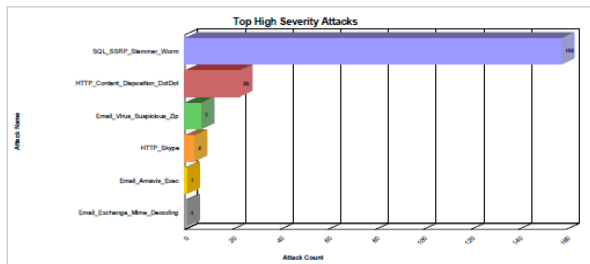
- **Top Attacks by Severity**

Neste relatório são mostrados os ataques de maior incidência (*top attacks*) por grupo de risco: alto, médio e baixo.

#### Top Attacks By Severity

Sorted By Count

Group Name: tupy  
 Period Start Time: 2009-09-02 0:00:00 GMT  
 Period End Time: 2009-09-02 23:59:59 GMT  
 Exceptions: Excluded  
 Subgroups: Included  
 Asset Type: All Assets  
 Includes: Intrusion Detection, AntiVirus, Network Anomaly Detection, Data Leakage Protection, Firewall



#### Top Attacks By Severity - (Continued)

Severity	Attack Name	Count	% of Subtotal	% of Total
High	SQL_SSRLP_Slammer_Worm	158	81.4%	8.1%
High	HTTP_Content_Disposition_DotDot	23	11.9%	1.2%
High	Email_Virus_Suspicious_Zip	7	3.6%	0.4%
High	HTTP_Skype	4	2.1%	0.2%
High	Email_Amavis_Exec	1	0.5%	0.1%
High	Email_Exchange_Mime_Decoding	1	0.5%	0.1%
Subtotal		194	100.0%	9.9%
Medium	Cross_Site_Scripting	1100	65.9%	56.4%
Medium	Email_Executable_Extension	467	27.4%	23.4%
Medium	HTTP_repeated_character	69	4.1%	3.5%
Medium	HTML_XSS_Attempt	35	2.1%	1.8%
Medium	PE_Overlapping_Header	6	0.4%	0.3%
Medium	Email_ReplyTo_Executable	1	0.1%	0.1%
Subtotal		1668	100.0%	85.5%
Low	ActiveX_Detected	53	60.2%	2.7%
Low	BitTorrent_DHT_Ping	35	39.8%	1.8%
Subtotal		88	100.0%	4.5%
Grand Total		1950	100.0%	100.0%

Figura 11 – Relatório de *Top Attacks*

- **Asset Event Details**

Mostra de forma detalhada quais foram os eventos e vulnerabilidades em um determinado período. Neste tipo de relatório são gerados centenas de linhas devido à quantidade de vacinas.

## Asset Event Details

#### Sorted By Owner

Group Name: tupy  
 Period Start Time: 2009-08-01 14:17:13 GMT  
 Period End Time: 2009-09-08 14:17:13 GMT  
 Exceptions: Excluded  
 Subgroups: Included  
 Asset Type: All Assets  
 Event Types: Intrusion Detection, AntiVirus, Firewall, Network Anomaly Detection, Data Leakage Protection

Attack Name	Owner	Tag	Criticality	Function	Count
ActiveX_Detected	Unassigned	143.166.83.24	Unassigned	Unassigned	1
ActiveX_Detected	Unassigned	161.58.160.102	Unassigned	Unassigned	1
ActiveX_Detected	Unassigned	168.75.225.44	Unassigned	Unassigned	5
ActiveX_Detected	Unassigned	172.16.1.7	Unassigned	Unassigned	1
ActiveX_Detected	Unassigned	172.16.100.10	Unassigned	Unassigned	4

Figura 12 – Relatório de eventos e vulnerabilidades

- **Top Attacks**

Utilizado para mostrar quais tipos de ataques tiveram maior incidência, ou seja, quais técnicas foram mais utilizadas dentro de um período de tempo.

## Top Attacks



### Sorted By Count

Group Name: tupy  
Period Start Time: 2009-09-03 0:00:00 GMT  
Period End Time: 2009-09-03 23:59:59 GMT  
Exceptions: Excluded  
Subgroups: Included  
Asset Type: All Assets  
Event Types: Intrusion Detection, AntiVirus, Firewall, Network Anomaly Detection, Data Leakage Protection

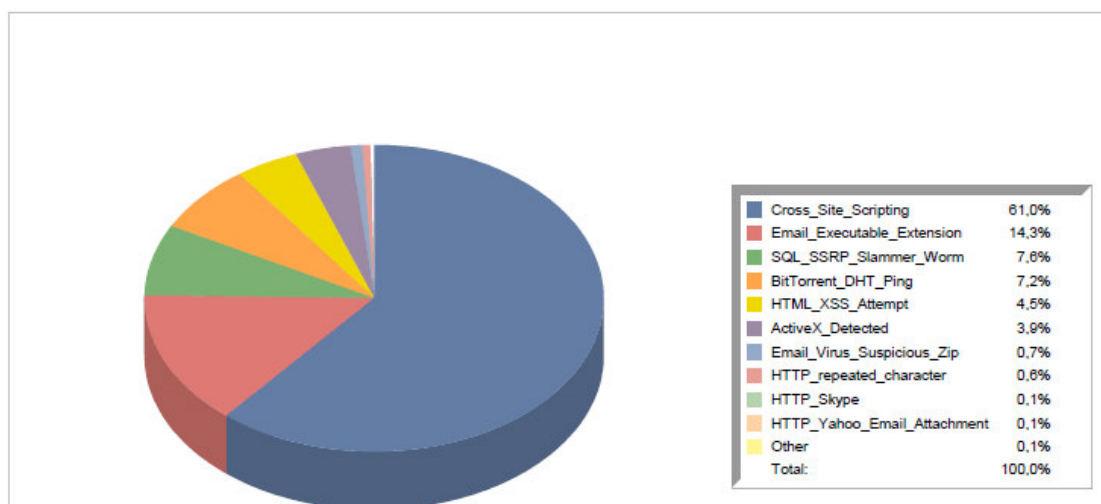


Figura 13 – Relatório de ataques por nível de incidência

## 9 Estratégia para implantação na empresa

Para que não houvesse impacto algum na empresa, inicialmente configuramos a solução em modo *inline simulation* por dois meses, analisando então o comportamento de todos os filtros e vacinas. Após esta análise, sabíamos exatamente quais vacinas poderíamos habilitar para fazer o bloqueio, detecção e quais não seriam relevantes habilitarmos para não causar uso de processamento indevido e espaço em banco de dados desnecessário. Deixamos a solução em rede trabalhando por mais dois meses para então elaborarmos a estratégia de instalação dos IPS/IDS de *host*. Fizemos inicialmente a instalação dos agentes de IPS/IDS de *host* em dois servidores, *DNS* e *Proxy Cache*, apenas em modo *inline simulation*. Após um mês habilitamos então os filtros de vacinas e auditoria ideais em nosso ponto de vista.

A implementação da solução em rede e *host* foi considerada tranqüila, porém mais demorada, pois efetuamos todos os procedimentos para que não houvesse impacto algum. Todos os *patches* e vacinas são aplicados e estudados caso a caso, visando sempre boa performance, espaço em banco de dados e impacto na rede corporativa. Com exceção de algumas regras de auditoria a percepção pelos usuários foi zero.

## 10 Considerações finais

Após instalação desta solução, pudemos ter uma visão mais clara de todas as ameaças ao qual estávamos sofrendo, estando agora em uma situação mais confortável.

Tínhamos muitos problemas com ataques de *DoS* (negação de serviço), ficando inacessíveis por muitas horas, bem como ataques de *SQL*, ao qual os atacantes tentavam, se

aproveitar de sessões abertas no banco de dados, sendo agora protegido pela solução de IPS/IDS.

Estamos certos de que fizemos a escolha correta, pois além de uma ótima solução de segurança, contamos com uma equipe especializada em detecção de ameaças e elaboração de vacinas e *patches* de segurança.

Devido às diversas ameaças cada vez mais frequentes na internet, entendemos que a única forma de as empresas protegerem seus negócios, é investindo cada vez mais em soluções de segurança, e claro, criar políticas de segurança eficazes, aplicando a toda corporação.

## **Bibliografia**

[1] SANS Institute - Network IDS & IPS Deployment Strategies. Disponível em: [http://www.sans.org/reading\\_room/whitepapers/intrusion/network\\_ids\\_ips\\_deployment\\_strategies\\_2143](http://www.sans.org/reading_room/whitepapers/intrusion/network_ids_ips_deployment_strategies_2143)

[2] RAMOS, Anderson et al. **Modulo Security Officer – Guia Oficial para Formação de Gestores em Segurança da Informação**. Porto Alegre: Editora Zouk, 2007.

[3] ZHANG, Xinyou; CHENGZHONG LI, Wenbin Zheng. **Intrusion Prevention System Design**. 2004 International Conference on, p. 386-390, set. 2004.

[4] ENDORF, Carl F; SCHULTZ, Eugene; MELLANDER, Jim. **Intrusion Detection & Prevention**. Estados Unidos: McGraw-Hill Professional, 2003.

[5] IBM - Providing preemptive protection for the network perimeter. Disponível em: [http://www-935.ibm.com/services/us/iss/pdf/ips\\_gx4004\\_datasheet.pdf](http://www-935.ibm.com/services/us/iss/pdf/ips_gx4004_datasheet.pdf)

[6] Proventia IPS G GX User Guide. Disponível em: [http://documents.iss.net/literature/proventia/ProventiaIPS\\_G\\_GX\\_User\\_Guide.pdf](http://documents.iss.net/literature/proventia/ProventiaIPS_G_GX_User_Guide.pdf)

[7] IBM Proventia Management SiteProtector Configuration Guide. Disponível em: [http://documents.iss.net/literature/SiteProtector/sp\\_configuration\\_guide20sp80.pdf](http://documents.iss.net/literature/SiteProtector/sp_configuration_guide20sp80.pdf)