CENTRO UNIVERSITÁRIO DE BRASÍLIA – UNICEUB

WOLMER ANDRADE GODOI

SISTEMA DE PREVENÇÃO DE INTRUSÃO APLICADO À ANÁLISE FORENSE

Brasília – DF
2006

WOLMER ANDRADE GODOI

SISTEMA DE PREVENÇÃO DE INTRUSÃO APLICADO À ANÁLISE FORENSE

Trabalho apresentado à Banca Examinadora da Faculdade de Ciências Exatas e Tecnologia – UniCeub, para conclusão do curso de Engenharia da Computação.
Orientador: Prof. M.Sc. Fabiano Mariath D´Oliveira.

Brasília – DF
2006

WOLMER ANDRADE GODOI

SISTEMA DE PREVENÇÃO DE INTRUSÃO APLICADO À ANÁLISE FORENSE

BANCA EXAMINADORA

_____

M.Sc. Fabiano Mariath D´Oliveira

_____

Marco Antônio de Oliveira Araújo

Brasília, 29 de junho de 2006.

“Dedico esse trabalho a minha família, em especial aos meus pais que, além de contribuir, de todas as maneiras possíveis, sempre e em tudo que eu precisei, insistiram, persistiram e não desistiram.”

AGRADECIMENTOS

Agradeço por ter a quem agradecer.

Agradeço a Deus sobre todas as outras coisas, pela vida, pelo mundo e a existência eterna.

À minha família, principalmente meus pais e irmãos, pelo apoio incondicional. Sempre presentes e pacientes!

Aos colegas do trabalho, meu sincero agradecimento pela paciência com as minhas angústias e, muitas vezes, com minha "ausência mental" – sempre preocupado com as atividades acadêmicas.

A Fernando Batelli, pelos constantes ensinamentos sobre postura de vida e retidão profissional.

À PSN Security, que permitiu meu acesso a tecnologia de prevenção de intrusão, somando no meu progresso e melhoria profissional.

Ao M.Sc. Paulo de Tarso Costa de Souza, pelo tempo investido nas conversas sobre mineração, extração e tratamento de dados.

À Dra. Isabel Grande e ao Dr. Augusto Maranhão, pelas revisões e discussões acaloradas sobre as questões legais.

Ao exemplo de mãe e mulher, Edivan Ismael dos Santos e à minha amiga-trunfo do coração, Maine Virginia Carvalho, o meu agradecimento pelas conversas noturnas, contra-argumentações sobre o texto e na forma de abordar cada uma das tecnologias deste projeto.

Aos colegas e amigos que acreditaram. Principalmente aos amigos Danuzia Pinheiro, Fábio Martins, Luciano Benoni, Luís Burdino, Marcos Thompson e Tenille Moraes que, durante todo esse tempo, me apoiaram nas horas difíceis com conversas e pontos de vistas diferentes.

A todas as pessoas que de alguma forma, direta ou indiretamente, dificultaram ou atrapalharam minha jornada, pois sem elas perceberem me fortaleceu e incentivou a melhorar, melhorar e melhorar.

E, finalmente, mas não menos importante, eu agradeço a todos que acreditaram que eu iria conseguir e que com certeza entenderam a minha ausência ao longo dos últimos meses e durante vários outros períodos dessa caminhada.

RESUMO

A evolução dos sistemas de detecção de intrusão para os sistemas de prevenção é uma realidade. Novas linhas de pesquisas e o constante desenvolvimento em segurança da informação têm dia-a-dia contribuído para o amadurecimento destas soluções. O presente projeto trata da proposição de um modelo que define os requisitos de comportamentos e de componentes de *software* que os sistemas de prevenção de intrusão deveriam adotar para armazenar informações sobre ataques, o ataque em si e assegurar confiabilidade destas informações para o perito forense, por meio de certificação digital.

Palavras-chave: Intrusão, forense, chave-pública, PKI, IDS, IPS, prevenção, detecção, segurança, ICP-Brasil, ICP, criptografia, modelo, captura, invasão.

ABSTRACT

The evolution of the Intrusion Detection Systems to Prevention Systems is a reality. New research lines and the constant development in the information security field have been contributing constantly to the maturity of these solutions. This project proposes a model that defines procedures and software components that should be adopted by the Intrusion Prevention Systems in order to store digitally certified information about attacks and the attack itself, information that could be further used by the forensic analyst.

Keywords: Intrusion, forensics, public key, PKI, IDS, IPS, prevention, detection, security, ICP-Brasil, cryptography, model, capture, invasion.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE DIAGRAMAS

LISTA DE GRÁFICOS

GLOSSÁRIO

Appliance[1]	Equipamentos configurados para executar uma tarefa específica. Exemplo: *firewall*, quiosque multimídia, sistema de caixa registradora ou ainda um leitor de código de barras, as possibilidades são infinitas.
Backdoor[2]	Um *backdoor* é um método de acesso remoto fortuito a sistemas computacionais que, ignora tanto autenticação, quanto esquemas de segurança destes sistemas, envidando esforços para não ser detectado em inspeções casuais.
Buffer Overflow[2]	Estouro da pilha de memória, resultado do armazenamento em um *buffer* de uma quantidade maior de dados do que sua capacidade. Esse ataque pode resultar em acesso privilegiado à memória e execução de código.
Broadcast[1]	Termo utilizado para designar um sinal que é irradiado para uma grande área geográfica, exemplo: os sinais de TV. Numa rede de computadores, um sinal de broadcast é um aviso enviado simultaneamente para todos os computadores da rede.
Checksum[2]	Forma para checagem redundante, é uma medida simples para proteger a integridade dos dados em uma transação eletrônica, detectando erros em uma transferência remota ou na gravação de arquivos.
DAT[2]	Cassete de gravação digital apresentado pela Sony, *Digital Audio Tape*, nos finais dos anos 80 em concorrência com o formato DCC da Philips.
Firewall[2]	Dispositivo de rede que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra.
FTP[2]	Acrônimo de *File Transfer Protocol* (Protocolo de Transferência de Arquivos), protocolo desenvolvido para transferir arquivos de forma rápida e confiável pela Internet.
Gigabyte[2]	2^{30} bytes. Um byte é um dos tipos de dados integrais em computação. É usado com freqüência para especificar o tamanho ou quantidade da memória ou da capacidade de armazenamento de um computador, independentemente do tipo de dados lá armazenados.
Hash[2]	Seqüência binária gerada por um algoritmo de *hashing*, normalmente se apresenta em formato hexadecimal. Essa seqüência busca identificar unicamente um arquivo ou informação.
Honeypot/net[1]	Recurso de segurança preparado especificamente para ser sondado, atacado ou comprometido e registrar essas atividades. Já *Honeynet* é uma rede projetada especificamente para ser comprometida e utilizada para observar os invasores. Essa rede normalmente é composta por sistemas reais e necessita de mecanismos de contenção eficientes e transparentes, para que não seja usada como origem de ataques e também não alertar o invasor do fato de estar em uma *honeynet*.
HTTP[2]	*HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto) é um protocolo da camada de "Aplicação" do modelo OSI, utilizado para transferência de dados na Internet.
ICMP[2]	*Internet Control Message Protocol*, é um protocolo integrante do Protocolo IP, definido pelo RFC 792, é utilizado para fornecer relatórios de erros à fonte original, ou reportar erros do protocolo UDP.
ICP[2]	Acrônimo de Infra-estrutura de Chaves Públicas. Estrutura responsável por processos de autenticação e validação de documentos eletrônicos. Executam a mesma atividade que os Cartórios Notariais.
IDS[2]	Acrônimo de *Intrusion Detection System*, sistema de detecção de intrusão é um dispositivo de rede, que trabalha verificando o tráfego de rede contra ataques e tentativas de invasão.
IETF[2]	*Internet Engineering Task Force*, é uma comunidade internacional ampla e aberta (técnicos, agências, fabricantes, fornecedores, pesquisadores) preocupada com a evolução da arquitetura da Internet e seu perfeito funcionamento. A IETF tem como missão identificar e propor soluções a questões/problemas relacionados à utilização da Internet, além de propor padronização das tecnologias e protocolos envolvidos.
IMAP4[2]	*Internet Message Access Protocol* é um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3.

IP[2]	Acrônimo para *Internet Protocol*, é o protocolo sob o qual assenta a infra-estrutura da Internet.
IPS[2]	Acrônimo de *Intrusion Prenvention System*, sistema de prevenção de intrusão é um dispositivo de rede, que trabalha em camada 2, de forma transparente, verificando o tráfego de rede protegendo-a contra ataques e tentativas de invasão.
IRC[2]	*Internet Relay Chat* é um protocolo de comunicação bastante utilizado na Internet. Utilizado para bate-papo (*chat*) e troca de arquivos, permite a conversa em grupo ou privada. É o predecessor dos comunicadores instantâneos (MSN, ICQ etc.).
Link[2]	Canal de comunicação de dados.
Log[2]	Termo para utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema, ou para que um administrador conheça o seu comportamento no passado. Um arquivo de *log* pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.
MP	Medida Provisória
OSI[2]	*Open Systems Interconnection*, ou Interconexão de Sistemas Abertos, é um conjunto de padrões ISO relativo à comunicação de dados. Um sistema aberto é um sistema que não depende de uma arquitetura específica.
POP3[2]	*Post Office Protocol* (POP3) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. O POP3 está definido no RFC 1225.
RFC[2]	Acrônimo de *Request for Comments*. É um documento que descreve os padrões de cada protocolo da Internet previamente a serem considerados um padrão. O processo de desenvolvimento de um RFC está também descrito na RFC 2026. Um documento-rascunho, o *Internet Draft* é proposto para o IETF e, após votação ou alteração, em que este se torna obsoleto devido à falta de interesse ou aceite, o documento revisto é publicado como um RFC.
SGBD[2]	Acrônimo para sistema de gerenciamento de banco de dados, é definido como o conjunto de programas de computador (*softwares*) responsáveis pelo gerenciamento de uma base de dados. Tem como principal objetivo retirar da aplicação cliente a responsabilidade de gerenciar o acesso, manipulação e organização dos dados. Disponibiliza interface para que seus clientes possam incluir, alterar ou consultar dados. Em bancos de dados relacionais a interface é constituída pelas *APIs* ou *drivers* do SGBD, que executam comandos na linguagem SQL.
Smart card[2]	Cartão que na maioria dos casos assemelha-se em forma e tamanho a um cartão de crédito convencional de plástico com tarja magnética. A grande diferença é que não possui tarja magnética e embute um microprocessador com memória que armazena diversos tipos de informação na forma eletrônica, com sofisticados mecanismos de segurança.
SMTP[2]	Acrônimo de *Simple Mail Transfer Protocol*, protocolo para envio de correio eletrônico definido pelas RFC 2821, 2822, 1869, 1891.
SNMP[2]	Do inglês *Simple Network Management Protocol* – Protocolo de Gestão Simples de Rede trabalha na camada de aplicação o que facilita o intercâmbio de informação entre os diversos dispositivos de rede. Trabalha sobre o protocolo UDP.
Socket[2]	Utilizado em ligações de redes de computadores para um fim de um elo bidirecional de comunicação entre dois programas. A interface padronizada de soquetes surgiu originalmente no sistema operacional Unix BSD (*Berkeley Software Distribution*).
SQL[2]	*Structured Query Language* – Linguagem de Consulta Estruturada é uma linguagem de pesquisa declarativa para banco de dados relacional (bases de dados relacionais).
SSH[2]	*Secure Shell* ou SSH é, simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota. Possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.
TCP[2]	Acrônimo para o inglês *Transmission Control Protocol*, é um dos protocolos sob os quais assenta o núcleo da Internet. Trabalha na camada de transporte (camada 4) do Modelo OSI, é confiável, orientado à conexão, ponto a ponto, com entrega ordenada e controle de fluxo.
Telnet[2]	Protocolo cliente-servidor de comunicações usado para permitir a comunicação entre computadores ligados numa rede, baseado em TCP.

Terabyte[2]	2^{40} bytes. Analogamente a uma unidade de medida, o byte e seus múltiplos operam para quantificar uma massa de dados em um sistema computacional.
TFTP[2]	Acrônimo de *Trivial File Transfer Protocol* (ou apenas TFTP) é um protocolo de transferência de arquivos pequenos, muito simples, semelhante ao FTP. Trabalha sobre o protocolo UDP e não possui mecanismos para autenticação ou criptografia de dados.
Tokens[2]	Hardware portátil que funciona como uma mídia de armazenamento. Em seus chips são armazenadas as chaves privadas dos usuários. O acesso às informações neles contidas é feito por meio de uma senha pessoal, determinada pelo titular. Assemelha-se a uma pequena chave e requer a utilização de uma porta USB, localizada, geralmente, na CPU do computador.
Throughput[2]	Vazão em um canal de comunicação de dados.
UDP[2]	Acrônimo do termo inglês *User Datagram Protocol*, faz a entrega de mensagens independentes, designadas por datagramas, entre aplicações ou processos. Protocolo leve, não-orientado a conexão, consequentemente não-confiável.
VoIP[2]	*Voice over IP* é a tecnologia que torna possível estabelecer conversações telefônicas em uma Rede IP (incluindo a Internet), tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.

Fonte: [1] www.guiadohardware.net
[2] www.wikipedia.org

1. INTRODUÇÃO

Os meios eletrônicos, sobretudo a Internet, possibilitam e facilitam a prática de vários crimes. O sentimento de anonimato, a impunidade e o alcance global dos meios de comunicação fazem com que o número de infratores dessa natureza cresça quase na mesma proporção que o avanço das tecnologias de comunicação [BLUM,2004]. Conforme estudo da IBM “A mudança na natureza do crime” [IBM,2006], publicado em abril de 2006, 71% dos executivos de TI no Brasil acreditam que o crime digital é mais custoso às suas organizações do que o crime físico. Em virtude disso, numa tentativa de garantir a segurança das informações e proteger seu patrimônio, gestores, diretores, gerentes e empresários investem vultosas somas de dinheiro nos mais variados dispositivos eletrônicos de segurança.

A necessidade de proteção, comum e vital ao ambiente empresarial, aumenta, em muito, o grau de dificuldade do processo de administração dos parques computacionais. Isso acontece porque dispositivos especialistas para proteção são constantemente inseridos no ambiente tecnológico coorporativo. *Firewalls*, sistemas de detecção e prevenção de intrusão (IDS/IPS), *honeypots/nets*, infra-estrutura de chaves públicas e privadas, algoritmos criptográficos, antivírus, sistemas de biometria, *tokens*, são alguns exemplos das tecnologias utilizadas para tentar coibir a ação do possível infrator e, desta forma, imprimir garantia às transações. Entretanto, cada dispositivo de segurança gera um enorme volume de informações, tais como registro de tentativas bem sucedidas, tentativas mal sucedidas, erros de acessos, bloqueios, entre outros.

Um outro aspecto a ser destacado é o fato de que tecnologias para proteção da informação, em sua grande maioria, têm padrões próprios de registro e *log*, o que resulta num volume ainda maior de informação armazenada e na dificuldade do gerenciamento.

Além disso, os infratores utilizam diversos artifícios para atingir o intento, como por exemplo, técnicas de evasão e de engenharia social que,

apesar de darem à invasão características únicas, são de difícil identificação num registro de *log*.

Como é possível perceber, no caso de crimes cometidos por meios eletrônicos, faz-se necessário pensar em ações de prevenção que sejam eficazes, não apenas no sentido de garantir proteção, mas também no sentido de viabilizar os estágios seguintes: a identificação dos infratores e a documentação de material para fins de aplicabilidade de medidas judiciais cabíveis.

Seja pelas inúmeras tecnologias ou pelos *gigabytes* de registros de acessos, procurar informações sobre dada invasão em um dispositivo comprometido, remontar as ações do atacante, garantir a cadeia de custódia – autenticidade e não-violação das informações – são tarefas muito trabalhosas para um perito digital, e isto, de certa forma, acresce o tempo de investigação, análise e execução das ações que deveriam ser adotadas por ele.

Chega-se pois a uma questão crucial: qual seria a melhor forma de proteção eficaz que permita, além da prevenção, adquirir e selecionar informações pertinentes e não manipuláveis, as quais poderão, caso seja necessário, funcionar como documentação material para, judicialmente, atribuir responsabilidades e sanções?

Do ponto de vista da tecnologia, os chamados Sistemas de Prevenção de Intrusão (IPS) são atualmente um dos meios mais eficientes para detectar e prevenir ataques [CHACON,2004]. São sistemas que operam na camada de aplicação, fazendo análise do tráfego da forma mais completa e acurada possível.

A partir dessa tecnologia o desafio é modelar um componente de *software* de modo que este seja capaz de munir com eficiência um investigador digital de informações. Este projeto se propõe a elaboração de um modelo computacional que permita ao IPS, além de suas funções de

detecção e prevenção, selecionar e guardar as informações do tráfego para que, se necessário, sejam utilizadas como prova documental perante a Justiça Brasileira.

2. TECNOLOGIAS PARA PREVENÇÃO DE INTRUSÃO

Este capítulo apresenta os principais elementos, conceitos e tecnologias acerca dos Sistemas de Prevenção de Intrusão de rede.

2.1 INTRUSÃO

Palavra de origem latina (*invasione*), é definida no Aurélio como “ato ou efeito de invadir”, o Houaiss define como o “ato de penetrar (em local, espaço etc.), ocupando-o pela força”. No direito é definida como “crime que consiste na entrada, sem autorização, em estabelecimento de trabalho com o objetivo de prejudicar as atividades normais ou danificar o próprio estabelecimento”.

Em tecnologia da informação, a primeira definição foi feita em 1990:

> Intrusão é qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou do sistema.
>
> *Dowel e Ramstedt [HEADY,1990]*

De acordo com essa última definição, um ataque deverá ser considerado uma intrusão. A relevância da definição do termo intrusão se dá no sentido de facilitar o entendimento da ação ou das ações executadas pelos invasores, para, a partir disso, elaborar sistemas que permitam dificultar, coibir ou mitigar os efeitos de uma invasão.

No presente projeto, as palavras **invasão** ou **intrusão** deverão ser entendidas como menção a um “ataque bem sucedido”. E o termo **ataque** deve ser entendido como qualquer “tentativa de invasão”.

Seguindo essa linha de raciocínio, uma intrusão é sempre conseqüência de um incidente de segurança. Em outubro de 1998, Howard e Longstaff, pesquisadores do Sandia National Laboratories, publicaram um estudo [HOWARD,1998] definindo uma linguagem comum para incidentes de segurança. O quadro a seguir resume este estudo.

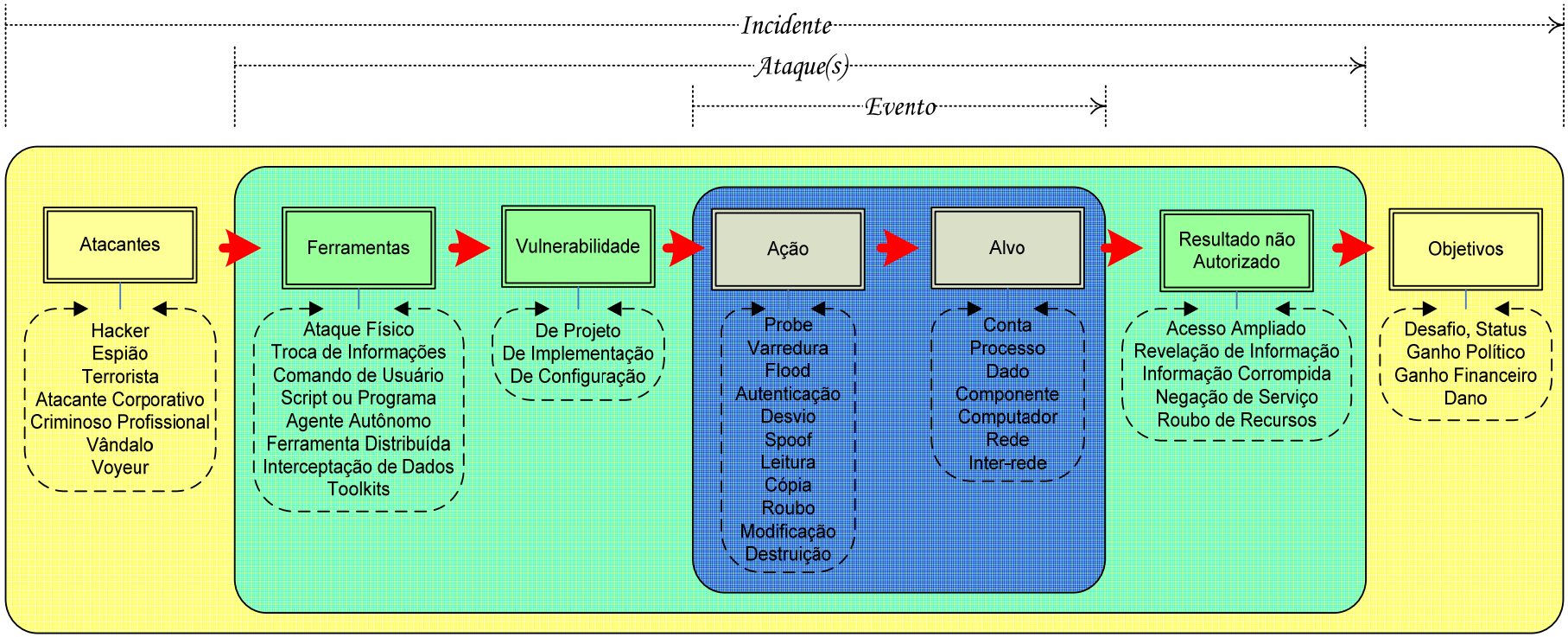


Figura 1 – Taxonomia de Incidentes de Segurança

As definições resultado do estudo foram muito bem aceitas na indústria de segurança computacional por descrever de forma clara a relação entre atacante e evento, segmentando objetivamente todos os passos de um incidente de segurança e fornecendo exemplos de cada etapa.

Todos os autores que escreveram sobre as classificações das intrusões, o fizeram com base na forma em que as intrusões são detectadas. A primeira classificação foi feita por Kumar [KUMAR,1995] que, em sua tese, classificou intrusões em duas classes principais, as quais são:

1. **Intrusão decorrida pelo mau uso do sistema ou detecção baseada em cenário** — ataques realizados a “pontos fracos” conhecidos do sistema. As técnicas de detecção buscam seqüências de ações nitidamente caracterizadas como inválidas, registradas em uma base de dados que contém o conhecimento acumulado sobre ataques específicos e vulnerabilidades do sistema.

2. **Intrusão decorrida pela mudança de padrão ou detecção baseada em anomalia** — são detectadas por meio da mudança do uso em relação a um padrão pré-definido do sistema. Traça-se, inicialmente, um padrão de comportamento, um perfil do sistema, e em seguida, por meio de monitoramento, procura-se por divergências significantes em relação a este perfil.

Métodos baseados em assinaturas (mau uso do sistema) dividem as ações possivelmente desempenhadas em “aceitáveis” e “não-aceitáveis”. Tomando por base diferentes fontes, como por exemplo, tráfego de rede ou *logs*, essas técnicas comparam as ações em andamento com o seu conceito de aceitável ou não e acionam o alerta para as violações [CAMPELLO,2001]. Como a intrusão ocasionada pelo mau uso segue padrões bem definidos, ela é facilmente detectada pela auditoria do sistema. Por exemplo, uma tentativa de criar um arquivo em uma pasta sem autorização pode ser detectada pela análise dos *logs* do sistema [KUMAR,1994].

Já a intrusão devido à mudança de padrão é detectada observando-se divergências significantes em relação à utilização normal do sistema. Pode-se construir um modelo a partir de valores derivados da operação do sistema [DENNING,1987].

2.1.1 Os passos de uma intrusão

Para os atacantes terem sucesso em suas investidas e executarem invasões bem sucedidas, é necessário que ele obtenha êxito em três pontos específicos: administração remota do servidor da vítima, acesso a este servidor quando necessário e finalmente, estas ações precisam passar despercebidas [JONES,2006].

Analisando as ações dos atacantes que lograram sucesso em suas investidas, Jones remontou as ações de invasão em cinco passos. Estes passos, apesar de não serem executados obrigatoriamente por todo invasor, são os mais comumente executados. Um computador que fique a mercê do invasor é conhecido como zumbi.

1º Passo – **Reconhecimento** – O intruso executa ações de reconhecimento contra o alvo para validar a conectividade, enumerar os serviços e checar a versão dos aplicativos servidores na busca de vulnerabilidades.

2º Passo – **Exploração** – Nessa etapa o intruso utiliza ferramentas para verificar a possibilidade de execução remota de código, escalação de privilégios ou condições para *buffer overflow*.

3º Passo – **Estabelecimento** – Nessa fase o intruso instala no servidor ferramentas para administração remota, usando aplicações de transferência de arquivos, tais como FTP, TFTP ou SCP. Para atingir seu objetivo o atacante pode escalonar privilégios no alvo ou explorar algum tipo de vulnerabilidade do *socket*. Após instalar suas ferramentas, estabelece um novo método para conectar ao servidor, popularmente conhecido como *backdoor*. Normalmente o atacante não utiliza a mesma vulnerabilidade para

acessar suas vítimas mais de uma vez. Pode ocorrer de o próprio atacante corrigir o problema no servidor da vítima para evitar que outros invasores se utilizem da mesma vulnerabilidade e se apoderem de "seu" servidor zumbi.

4º Passo – **Consolidação** – A ferramenta de *backdoor* pode trabalhar de três maneiras, a primeira, ela toma a forma de um serviço, permitindo que o atacante se conecte quando desejar, a segunda maneira, inversa a primeira, a ferramenta de *backdoor* se conecta ao computador do atacante gerando uma requisição de dentro da rede da vítima para fora. A terceira seria o servidor zumbi estabelecer uma conexão a uma rede de bate-papo (IRC) de onde o atacante daria os comandos para a *backdoor*. É nessa fase em que o atacante, normalmente, se cerca de cuidado para que não seja descoberto.

5º Passo – **Pilhagem** – Nesta última etapa o intruso executa a parte final do seu plano, que pode envolver o roubo de dados críticos, o possível estabelecimento de uma nova base para ataques ou qualquer outro ato, de acordo com seu intuito.

2.1.2 O intruso

De forma muito simplificada, o conhecimento comum define que um intruso é alguém que invade o sistema ou utiliza-o de forma indevida [OLIVEIRA,1999]. Mas cabem outras questões: como caracterizar um intruso? Um usuário que tenta acessar seu sistema várias vezes consecutivas e erra todas não intencionalmente pode ser classificado como um intruso? O que diferencia um usuário legítimo de um intruso? Ou ainda, quando um usuário legítimo se transforma em intruso?

Neste estudo, o intruso só pode ser caracterizado por suas ações. Afinal, como afirmou Aristóteles, “somos aquilo que fazemos” [ARIST,1973].

Como procedimento comum, para tentar diferenciar as ações legitimas das ações nocivas, os administradores de sistema definem um *threshold*, ou seja, uma quantificação mínima aceitável de dado comportamento antes que

tal ação seja considerada um ataque ou uma tentativa de invasão.

Dessa forma, os administradores personalizam um limite aceitável de erros que não serão considerados ataques, diferenciando assim o atacante e o intruso do usuário legítimo.

Oliveira [OLIVEIRA,1999] classificou os intrusos em dois tipos: externos e internos. Neste trabalho, o enfoque inicial será para os ataques de uma maneira geral e, num momento posterior tratará da intrusão de forma mais específica.

Para melhor compreensão do que venha a ser ataque externo, é necessário definir o que é ambiente interno e o que é ambiente externo. O primeiro é o local ao qual o responsável pela administração do parque tecnológico tem acesso físico e administração lógica. O ambiente externo é o local ao qual o responsável pela administração do parque tecnológico não tem acesso físico, nem administração lógica, dessa forma:

1. **Ataques Externos** — ataques originados do ambiente externo. Exemplo: ataques oriundos da Internet.

2. **Ataques Internos** — ataques originados do ambiente interno. Exemplo: ataques originados de dentro da corporação, provenientes de máquina contaminada por um vírus.

Segundo estudo feito no Brasil, publicado pela PricewaterhouseCoopers em julho de 2004 [ANDREA,2004], 87% das organizações brasileiras declaram que os ataques sofridos tiveram origem interna, sendo que 32% destas invasões foram efetuadas por empregados autorizados, 28% por empregados não autorizados e 27% por empregados desligados. Ou seja, 87% do total das invasões são efetuadas por pessoas mal intencionadas.

Para entender melhor a taxonomia da intrusão é necessário entender os agentes motivadores. Por isso, o foco recai no elemento humano, nas pessoas de uma maneira geral.

Surge, assim, uma questão: o que levaria uma pessoa a cometer um crime e, por conseguinte, se transformar em um criminoso? Não há uma resposta definitiva, mas é uma questão importante. Na análise forense um perito precisa responder a três elementos para que alguém seja responsabilizado por um crime: motivo, oportunidade e meio — MOM [HARRIS,2005].

Motivo seria "quem" e o "porquê" de um crime. Pode ser induzido por circunstâncias internas ou externas. Uma pessoa pode ser guiada pela excitação, pelo desafio ou pela adrenalina de cometer um crime. Esses são exemplos de motivadores internos. Já as circunstâncias externas podem incluir problemas financeiros, um membro da família doente ou situações de chantagem. Tentar compreender o motivo da ocorrência de um crime é parte importante para definir quem cometeria tal atividade. Atacar os motivadores que levam uma pessoa a cometer um crime é uma ação que, se posta em prática pelos agentes da segurança, diminuiria a incidência de crimes. Seria a ação no fator primário, na raiz do que poderia vir a ser o problema.

Oportunidade pode ser entendida como o "onde" e o "quando" de um crime. As oportunidades são geralmente ocasionadas por vulnerabilidades ou fraquezas não corrigidas. Se um agente de segurança descobre porque uma pessoa poderia desejar cometer um crime (motivo), ele poderá analisar quais seriam as situações (oportunidades) que possibilitariam o crime e desse modo tomar ações preventivas e evitar a ocorrência.

Meios podem ser entendidos como os caminhos ou formas através dos quais um criminoso pode vir a ter êxito em sua empreitada. Tal informação pode ser muito importante no sentido de identificação de um infrator. Por exemplo, num caso de um crime ocorrido contra uma instituição financeira, dependendo dos meios utilizados, é possível ao agente de segurança traçar de forma mais acurada um perfil do suspeito.

2.2 SISTEMAS DE PREVENÇÃO DE INTRUSÃO

O objetivo primário do Sistema de Prevenção de Intrusão — *Intrusion Prevention System,* em inglês, ou simplesmente IPS, é, como o próprio nome sugere, o de prevenir uma invasão. No âmbito tecnológico, os IPS previnem também todo e qualquer ataque.

De maneira simples, podemos afirmar que os IPS garantem a prevenção trabalhando da seguinte forma: primeiro interceptando a comunicação e, em seguida, atuando na remontagem do fluxo de dados. Uma vez remontado o fluxo, o IPS efetua sua análise a partir da camada de rede para a camada de aplicação e atua garantindo ou não permissão para aquele tráfego.

Para um IPS ser eficiente é preciso que seu subsistema de detecção seja tão eficiente quanto ele. Cabe, então, uma questão: como ele pode prevenir um ataque que não é detectado?

2.2.1 Sistemas de detecção de intrusão

2.2.1.1 Histórico

Voltemos pois à década de 70. Com a disseminação dos *mainframes* nos Estados Unidos, os usuários passaram a manipular os equipamentos sem a interferência do operador. Como conseqüência o risco de comandos indevidos e das tentativas de ataques ao sistema tornou-se um problema real. Em 1972, James P. Anderson, em seu relatório para Força Aérea Americana (USAF) [AND,1972], escreveu sobre os problemas de segurança no uso de *mainframes*. Em 1980, James apontou a necessidade de monitoramento de atividades contra mau uso dos sistemas de computação [AND,1980]. Esse último artigo foi o responsável pelo inicio das atividades de monitoramento contra o mau uso nos *mainframes*. Entretanto, essas atividades se limitavam a vistorias esporádicas nos arquivos de *log* do sistema [CAMPELLO,2001].

Só com o surgimento e a popularização das redes de computadores é que o estudo de detecção de intrusão obteve maior alcance. Cresceu a conectividade, cresceram os problemas com ataques e, conseqüentemente, cresceu também o investimento em técnicas e ferramentas para detecção rápida e automática de possíveis intrusões o qual evoluiu chegando aos IPS atuais.

Os então conhecidos como IDES — *Intrusion Detection Expert Systems* — evoluíram para IDS — *Intrusion Detection System*. O IDS agregou funcionalidades de alertas reativos, como por exemplo, envio de correio eletrônico quando detectava ataque. Ou seja, evoluiu para Sistema de Resposta de Rede Reativo ou IDS reativo que, em outras palavras, significa que, no caso de ataque, o dispositivo altera a configuração do *firewall* para bloquear o atacante, ou altera rotas no roteador.

A tecnologia de detecção de intrusão levou mais de 20 anos para chegar a seu patamar atual.

Cronologia

1972	James P. Anderson publica o primeiro estudo sobre segurança computacional para a Força Aérea Americana (USAF).
1980	James P. Anderson publica um estudo sobre o uso de logs de auditoria para detectar ações não autorizadas, classificando ameaças e sugerindo melhorias nos subsistemas de auditoria para mainframes;
1984-1986	Dorothy Denning e Peter Neumann pesquisaram e desenvolveram o primeiro modelo de um IDS de tempo real. Esse protótipo recebeu o nome de Sistema Especialista de Detecção de Intrusão (*Intrusion Detection Expert System* – IDES).
1985	É realizado entre o Laboratório de Ciência da Computação da SRI (*Stanford Research Institute International*) e a marinha norte-americana um contrato de pesquisa, objetivando a construção do sistema IDES. Um dos IDS's de maior influência nas futuras pesquisas da área, O IDES foi o primeiro IDS a combinar métodos estatísticos com técnicas baseadas em regras;
1987	Primeiro *Annual Intrusion Detection Workshop*, organizado pela SRI. Formado por vários pesquisadores da área com o intuito compartilhar informações;
1989	Nasce a detecção de intrusão em redes. Todd Heberlien, então estudante, escreve o *Network Security Monitor* (NSM), ferramenta que captura pacotes TCP/IP e detecta atividades anômalas em redes heterogêneas;

1994	Pesquisadores do Centro de Suporte Criptográfico da força aérea norte-americana criam o ASIM, o primeiro IDS de rede, e formam uma empresa (Wheelgroup) para comercializar a tecnologia de detecção de intrusão em rede;
1997	A Cisco adquire a Wheelgroup, tem início o programa de incorporação de detecção de intrusão à seus roteadores. A ISS (Internet Security Systems) lança o RealSecure, IDS distribuído para Windows NT, introduzindo novos conceitos no mercado de detecção de intrusão;
1998	É publicado o documento "*A Common Intrusion Detection Framework*". Uma tentativa de padronizar o funcionamento e tecnologias acerca de Sistemas de Detecção de Intrusão
1999	O governo norte-americano estabelece um programa de cooperação entre indústria e governo com o objetivo de aumentar o uso de IDSs e proteger a infra-estrutura nacional. A FIDNet (Federal Intrusion Detection Network) é criada com o intuito de detectar ataques à infra-estrutura de rede ligada a sites do governo norte-americano.
2000	O IETF (Internet Engineering Task Force) cria o grupo de trabalho para definir um protocolo de troca de mensagens entre dispositivos detectores de intrusão, o IDWG (Internet Detection Working Group).
2001	Surge o conceito de prevenção de Intrusão. O Gartner Group publica: "Intrusion Detection is dead, Intrusion Prevention is the future."
2003	Neil Desai publica para o site *SecurityFocus* o artigo "Intrusion Prevention Systems: the Next Step in the Evolution of IDS". Esse artigo definiu o funcionamento e características dos Sistemas de Prevenção de Intrusão.
2006	O IDWG conclui seus trabalhos gerando três *internet-drafts* ((*Intrusion Detection Mesage Exchange Requirements, The Intrusion Detection Message Exchange Format* e o *the Intrusion Detection Exchange Protocol (IDXP)*), estando em estudo para aprovação como padrão e posterior definição como RFC.

Tabela 1 – Cronologia dos Sistemas de Detecção e Prevenção de Intrusão

2.2.1.2 Funcionamento dos sistemas de detecção de intrusão

A maioria dos Sistemas de Detecção de Intrusão de rede pode ser configurada com duas placas de redes, uma para o gerenciamento e a outra para detecção (Figura 2). A placa de rede configurada para detecção normalmente não tem endereçamento IP — *Internet Protocol*, o que faz com que ela fique invisível. Uma vez que ela não tem endereço IP não pode interagir com a rede, ou seja, não há envio de pacotes.

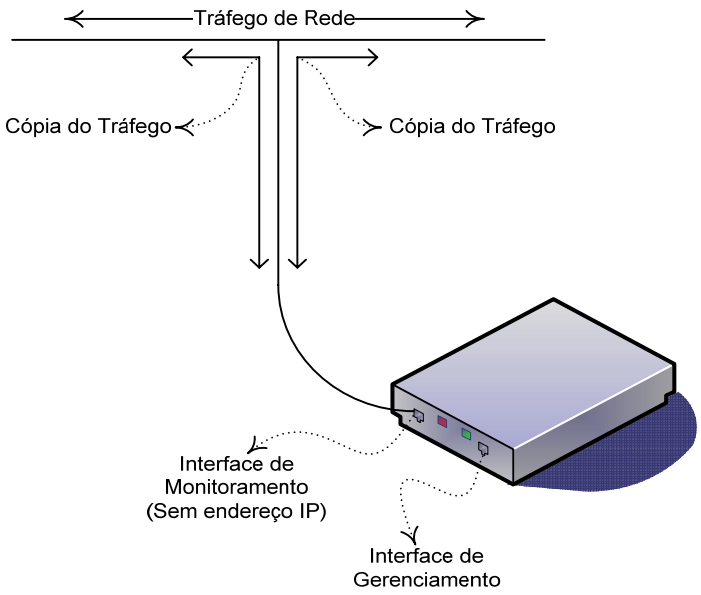


Figura 2 – Esquema de Funcionamento de um IDS

O dispositivo é meramente informativo e não influencia no tráfego. Nesse tipo de dispositivo, o monitoramento é feito somente no tráfego que entra, ou seja, no tráfego que chega até a porta de monitoramento. Para que o dispositivo funcione, no entanto, ele depende do concentrador da rede — um *hub* ou um *switch*. No caso do segundo, é necessária a capacidade de espelhamento de porta.

Esse tipo de dispositivo possui claros problemas de *throughput* na captura. Na grande maioria dos dispositivos de detecção de intrusão, a porta de monitoramento possui uma limitação física de, no máximo, 100 Mbps. Já nos dispositivos que possuem porta com maior capacidade, a limitação física é de 1Gbps. Pelo concentrador podem passar 2.4 Gbps, ou seja, vinte e quatro vezes a capacidade máxima da porta de monitoramento no caso mais comum (100Mbps); ou 1.4 vezes no caso do dispositivo com porta de maior capacidade. A implicação direta dessa limitação é a de que nem todo tráfego é analisado, o que significa que ataques podem passar despercebidos pelo dispositivo de detecção de intrusão.

Comparando essa estrutura a uma rede de distribuição de água seria como dizer que a demanda de uma cidade é maior que a capacidade de análise da qualidade da água tratada. Ou seja, a cidade será abastecida, entretanto

não há meios de garantir que toda a água estará com qualidade satisfatória para o consumo.

Cientes desse problema, os desenvolvedores das soluções de detecção de intrusão alteraram o funcionamento do dispositivo para que o mesmo ficasse em linha, ou seja, ficasse diretamente no caminho em que o pacote precisa passar para chegar a seu destino (figura 3). Como exemplo de um dispositivo em linha, pode-se citar o roteador.

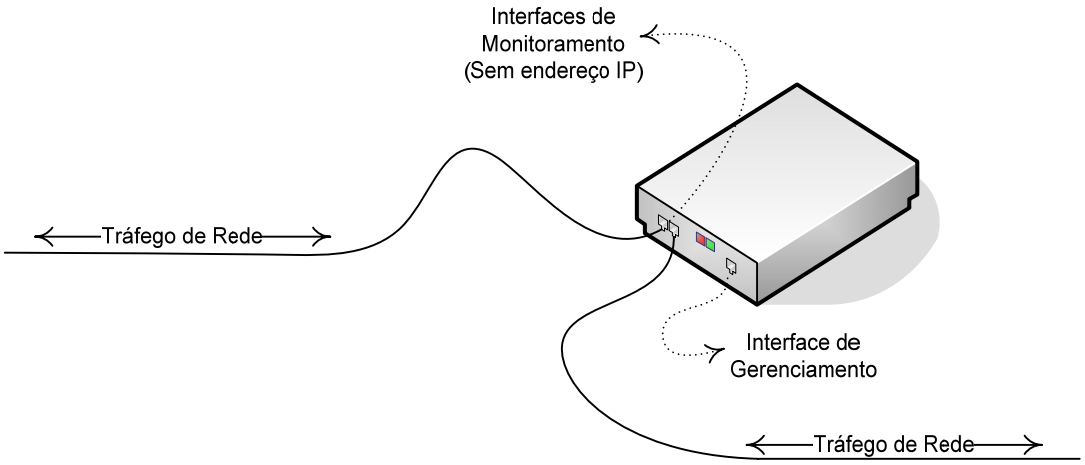


Figura 3 – Esquema de funcionamento de um IPS em linha

Esse tipo de implementação permitiu que todo tráfego fosse monitorado. Concomitantemente, outras características foram adicionadas aos IDS; envio de TCP *reset*, ou ICMP *Host Unreachable*, reconfiguração das regras do *firewall*, ou alteração de configuração no roteador (regra de bloqueio ou alteração de rota utilizando ACL) são alguns exemplos de resposta a ataques. Com essa melhoria alguns autores passaram a definir os IDS como sistema de detecção de ataque de rede com resposta ativa. Pois em vez de simplesmente informar o ataque, o dispositivo, no caso de detecção de um ataque, toma uma ação ativa em relação ao tráfego. Esse tipo de abordagem dos IDS é, entretanto, somente mais uma designação para os IDS reativos.

2.2.2 Características dos sistemas de prevenção de intrusão

A característica que faz do IPS um sistema de bloqueio pró-ativo é a sua disposição privilegiada na rede. O IPS é um dispositivo em linha, com análise em camada de aplicação. Essa maneira de funcionamento permite que ele aja como um porteiro, autorizando ou bloqueando o tráfego de maneira mais detalhada e eficiente.

Outro ponto importante é o fato das interfaces de monitoramento não possuírem endereçamento IP. Dessa forma, o dispositivo funciona como uma ponte em camada 2 (*bridge*). Essa característica garante que o próprio dispositivo não sofra ataques de evasão. Ataques de evasão são ataques para “enganar” ou burlar um dispositivo de detecção de intrusão.

Várias tecnologias de análise de dados na camada de aplicação foram desenvolvidas. A tecnologia *Deep Packet Inspection* é hoje a que reúne mais elementos para análise de pacotes. Essa tecnologia é definida e implementada por vários fabricantes de maneiras diferentes. Para evitar erros, neste trabalho assume-se a tecnologia *Deep Packet Inspection* como a união da remontagem do fluxo de dados com inspeção da tabela de estado das conexões TCP.

Vários fabricantes adicionaram a tecnologia *Deep Packet Inspection* em seus *firewalls*, entretanto um *firewall* com essa tecnologia deixa muito a desejar quando comparado a um IPS. Primeiro, pela necessidade que o *firewall* tem de tratar o pacote para roteá-lo; segundo, pela característica inicial que um *firewall* apresenta: a de ser a primeira camada de proteção efetiva na proteção de uma rede.

O esquema mais eficiente de segurança é a segurança em camadas. É o esquema de segurança que se utiliza na vida real. Para visualizar o que está sendo afirmado podemos usar uma imagem presente em alguns romances da Idade Média. Quando se desejava proteger algo valioso, este bem era guardado em um cofre trancado, colocado em uma torre, de difícil acesso –

feito por escadas gigantescas – e essa torre era, via de regra, um cômodo de castelo com muro alto e sentinelas, de preferência cercado por um fosso com jacarés.

A cena do exemplo pode ser pitoresca, mas é ideal para se falar em segurança em camadas. Fazendo ainda um paralelo com essa estrutura da Idade Média, o roteador com ACL´s (*Access Control Lists*) seria a primeira camada do “fosso com jacarés”; em seguida o *firewall stateful* com regras e manutenção da tabelas de estado seria “o muro alto com sentinelas”; e por último, um IPS seria a “torre, de difícil acesso – feito por escadas gigantescas” e ainda o “cofre”.

A interação que os IPS têm com a camada de aplicação dos pacotes é seu maior diferencial. Apesar de existirem outros dispositivos com tecnologia para análise de fluxo de dados em camada de aplicação, nenhum reuniu de forma tão eficiente técnicas de detecção de intrusão, fazendo análise da camada de rede à camada de aplicação.

2.2.3 Técnicas para detecção de ataques

Comparando-se um dispositivo de detecção de intrusão ao corpo humano, pode-se dizer que a capacidade de processamento seria o coração, e o algoritmo de detecção, o cérebro. Utilizando os dados coletados, o dispositivo deverá processar e analisar todo esse tráfego, usando vários algoritmos para identificar e reagir ao ataque. Existem várias técnicas e algoritmos de análise.

As técnicas usadas para analisar o tráfego de dados buscando detectar intrusões podem ser classificadas em dois grupos: detecção por mau uso ou cenário, e detecção por comportamento ou anomalia [TAVARES,2002].

A detecção por cenário trabalha comparando regras (seqüência de ações) pré-estabelecidas no tráfego da rede com uma base de padrões (assinaturas) de ataques conhecidos; é uma técnica comparativa.

As técnicas de detecção por cenário são também conhecidas como *pattern matching*:

a) ***Pattern matching*** – É uma técnica utilizada por dispositivos de detecção de intrusão para detectar ataques utilizando base de assinaturas.
   Essa técnica é a forma mais simples e mais utilizada de se detectar um ataque, entretanto possui limitações. A engenharia da técnica se baseia na comparação do pacote capturado, com uma seqüência de texto ou uma seqüência binária; ou seja, procura por assinaturas conhecidas de ataques. Um IDS usando detecção por assinatura precisa de atualização contínua das assinaturas mais novas, para que possa detectar os ataques atuais. É necessário ainda manter um trabalho constante de pesquisa para criar essas novas assinaturas.
   Uma simples mudança no esquema de ataque pode ser suficiente para "enganar" um IDS, pois a assinatura não será mais coincidente. *Pattern matching* é considerada uma técnica muito rápida na detecção de ataques. Todavia, isso pode deixar de ser verdade, pois as assinaturas de ataques contêm conjuntos crescentes de regras. Se somarmos isso ao constante crescimento do link – mais tráfego para analisar – teremos como resultado um crescimento indefinido da utilização da capacidade de processamento, de modo que essa técnica pode se tornar impraticável.

A técnica *pattern matching* é reativa, funciona como em um antivírus. O criminoso cria o vírus, o vírus se dissemina, as empresas de antivírus criam a vacina e a partir daí os sistemas de antivírus conhecem o ataque e passam a fazer a proteção.

Um outro grupo de técnicas é a detecção por comportamento. Conhecida também como detecção por anomalia, age quando os dados coletados são comparados com dados previamente obtidos quando do comportamento normal do sistema. Desvios da normalidade são então tratados como ataques.

a) **Análise de Protocolo** – A necessidade do desenvolvimento de uma

assinatura para cada novo ataque obrigou os pesquisadores a procurar diferentes métodos para detecção de ataques novos ou desconhecidos.

A análise de Protocolo é a técnica de detecção de intrusão que verifica o uso inadequado do protocolo. Para isso requer o modelo descritivo do uso convencional do protocolo. Os protocolos são definidos por RFC (*Request for comments*) e outros documentos normativos. Essa técnica prega que qualquer uso do protocolo fora de sua especificação deve ser considerado como anormal. Assim como no *pattern matching*, a análise de protocolo trabalha com assinatura e cada conjunto de assinaturas pertence a um determinado protocolo. A utilização de análise de protocolo é mais eficiente tanto na detecção de ataques conhecidos, como de desconhecidos. Com o foco em anomalias no tráfego em vez de simplesmente verificar assinaturas de um ataque em particular, a engenharia deste algoritmo dificulta exponencialmente as tentativas de evasão utilizadas pelos criminosos virtuais.

Técnicas de evasão, conforme explicado anteriormente, podem ser definidas como ações que atacantes virtuais tomam para passar por dispositivos de detecção de intrusão de forma a não serem percebidos.

Na detecção por protocolo apesar da necessidade do desenvolvimento de assinaturas específicas por protocolo, ela é classificada como uma técnica “comportamental”, pois, qualquer diferenciação, anomalia, do uso do protocolo será percebida pelo dispositivo de detecção e gerado um alerta relativo à alteração.

b) **Abordagem probabilística e estatística** – A abordagem probabilística oferece um poderoso complemento à abordagem baseada em assinatura. A maioria dos desenvolvedores de sistemas de prevenção de intrusão utiliza-se de redes bayesianas para os módulos de detecção por probabilidade. Sistemas bayesianos desenvolvem um conhecimento não baseado em termos de regras ou assinaturas, mas um conhecimento por relacionamentos probabilísticos condicionais. Com essa ação, eles ganham muito da sensitividade e especificidade dos sistemas baseados

em assinaturas, bem como retêm muito da habilidade dos sistemas de detecção baseados em anomalias.

A engenharia desta técnica funciona da seguinte forma, inicialmente são coletados e analisados dados da rede; durante essa fase são marcados, tanto ataques reais quanto falsos positivos que entram em um modelo estatístico; após o acúmulo de um volume considerável de dados, sistemas bayesianos são utilizados e padrões tomam forma no modelo. Os padrões revelam, por meio de análises estatísticas, qual tráfego é um falso positivo e qual tráfego é realmente um ataque malicioso. Estes padrões são então aplicados a novos fluxos do tráfego da rede. Os padrões aprendidos prevêem indicadores mais precisos entre falsos positivos e tráfego malicioso, reduzindo significativamente o número de falsos positivos identificados pelo IDS. É importante destacar que como os IDS baseados em estatísticas precisam primeiro aprender o que é um tráfego normal, eles são pouco efetivos na defesa da rede no período inicial de seu funcionamento. Um outro problema é que durante o período de aprendizado (*learning mode*) o tráfego da rede precisa ser livre de ataques. Diante disso surge a questão: como garantir isso com 100% de certeza?

c) **Redes neurais** – Utilizam técnicas de aprendizado adaptativo para reconhecer comportamento anormal. Isto ocorre porque redes neurais não precisam de parâmetros definidos pelo usuário. A rede neural precisa, primeiro, ser treinada com tráfego limpo, ou seja, tráfego não contaminado com atividades maliciosas. O sistema precisa estar em treinamento contínuo, permitindo que a rede neural absorva as mudanças no comportamento do tráfego. Por causa da habilidade de aprender, elas são valiosas para apontar anormalidades. Todavia, redes neurais não podem ser utilizadas para determinar a causa da anormalidade. Elas podem somente determinar se existe uma violação de segurança, mas não sua causa. O esforço adotado para contornar este problema é o desenvolvimento de redes neurais especializadas em um só tipo de ataque. Isso torna seu uso extremamente eficiente para

detecção de intrusão, todavia, essa tecnologia atualmente fica restrita a laboratórios de pesquisa e não existe solução comercial implementada no ambiente corporativo.

Técnicas de detecção por anomalia, apesar de se encontrarem em um estágio inicial, já são realidade nas soluções comerciais. Já as Tecnologias de Detecção de Intrusão, apesar do longo período de desenvolvimento e do maciço investimento da indústria de segurança, ainda têm muito para evoluir. Existem trabalhos publicados com propostas das mais diversas para desenvolvimento de algoritmos com novas abordagens para detecção de intrusão.

A proposição teórica destes algoritmos pode ser considerada como passo inicial para desenvolvimento das tecnologias que estão por vir, demonstrando claramente a necessidade de melhoria e o investimento na tecnologia dos dispositivos de detecção de intrusão.

A seguir alguns exemplos destas proposições:

a) **Detecção estrita de anomalias** – Essa técnica de detecção em vez de usar um grupo de assinaturas para detectar uma intrusão, efetua busca por variações comparando o tráfego com uma definição restrita do uso. A grande vantagem de se utilizar esse modelo é que o número de regras do grupo de “mau uso” nunca poderá ser maior que o número de regras de ataques de "não uso"; pois, por definição, todos os ataques atuais e futuros estarão no grupo de regras de "não uso". Um dos pontos mais interessantes é que um IDS que implementa essa técnica não emite falsos positivos, ou seja, ele nunca gera um falso alarme, pois a atividade que ocorre fora da definição do uso, por definição, é relevante sob o ponto de vista de segurança. A dificuldade em construir um IDS que utiliza um modelo de detecção estrita das anomalias é exatamente na definição do uso aceitável. Esse tipo de abordagem pode ser muito bem empregado em um ambiente no qual o uso dos recursos de rede pode ser, ou já é, muito bem definido.

b) **Análise holística** – A abordagem holística é considerada como o oposto da visão convencional de segurança [SASHA,2003]. A análise convencional é também chamada de análise reducionista. Ela consiste na análise em baixo nível como um indicador de uma intrusão. Holismo é baseado na crença que o todo é maior que a soma de suas partes, ou seja, o todo é indivisível, inseparável. Traduzindo isso numa abordagem de segurança, significa dizer que é possível inferir na existência de um ataque quando um grupo de observações (ainda que superficialmente não pareça correlacionado) possa ser relacionado, mesmo de forma aproximada, à uma estrutura que representa o conhecimento de um método que um ataque emprega em alto nível. Em outras palavras, os métodos reducionistas geram uma suposição de verdade baseada na observação de uma ação particular (abordagem *botton-up*). Já os métodos holísticos têm sua engenharia de forma inversa. O método parte de um conhecimento geral para deduzir uma observação específica (abordagem *top-down*). Existem varias maneiras de se implementar análise holística, um exemplo seria fazer uma trilha, de forma que o nó principal da rede atue como a barreira final que precisaria ser transposta para um atacante alcançar seu objetivo. Outra opção seria observar de forma global quais são as táticas que o atacante usa e utilizar a observação para deduzir a próxima tática que poderá ser utilizada para atacar. É necessário salientar que o modelo holístico se baseia em dados coletados em um ambiente usando métodos reducionistas, logo, é um método dependente e que precisa ser utilizado em conjunto com o método reducionista.

c) **Algoritmos genéticos** – Algoritmos genéticos trabalham da mesma forma que a Teoria Evolucionária de Darwin associada à engenharia genética [LI,2005]. Atualmente, algoritmos genéticos podem ser utilizados para resolver uma grande gama de problemas. Eles procuram uma solução "boa suficiente" em vez da "melhor" solução. A idéia é transformar toda solução de um problema em um "código genético" que deve ser pontuado por uma função de avaliação. E quando essa

pontuação não é suficiente o código é rejeitado. De forma concreta, é necessário que seja gerado um número mínimo de soluções de "código genético". Esse conjunto de “códigos genéticos” é chamado de "população" e essa “população” é então avaliada em relação ao problema. Se alguns destes códigos forem bons o suficiente, tudo bem. Caso não, os melhores códigos são selecionados, recombinados (a recombinação é feita pela troca de pontuação entre os códigos, dependendo do tipo da solução) e sofrem mutação (algoritmo de randomização) para então serem reavaliados. No caso particular dos IDS, esses algoritmos, podem, por exemplo, ser utilizados para ajudar na criação de conhecimento para um Sistema Baseado em Regras (RBS – *Rule Based System*). A maior dificuldade está em encontrar a maneira correta de traduzir a solução em um esquema genético e definir qual é a melhor função de avaliação para se utilizar.

d) **Algoritmos de biotecnologia** – Algoritmos de biotecnologia são utilizados para detectar ataques mascarados [COULL,2003]. Ataques mascarados ocorrem quando o atacante rouba uma seção TCP legítima. Essa abordagem prega a aplicação do algoritmo de determinação da similaridade entre DNA´s ou seqüências protéicas, para efetuar detecção de intrusos. A precisão dos resultados de comparação de DNA e a flexibilidade desses algoritmos em serem modificados para uso em diferentes aplicações, torna-os muito atrativos para uso em sistemas de detecção de intrusão, um exemplo de uso seria a substituição das seqüências de nucleotídeos pela coleção de comandos de usuários. Isto é feito da seguinte forma: adota-se que os comandos de entrada do usuário são “pegadas digitais" deste usuário. Este algoritmo é capaz de aliar e associar as seqüências dos comandos de inúmeras maneiras. Um resultado típico com 75% de acerto possui uma taxa de erros de 7,5%. O acerto ocorre quando uma ação intrusiva é identificada corretamente, o erro é também chamado de falso positivo e ocorre quando uma ação válida no sistema é identificada como intrusão. Esse tipo de abordagem não é o melhor resultado para detecção de intrusão no tráfego de uma

forma geral. Mas observando ataques mascarados o resultado pode ser considerado muito bom.

e) **Algoritmos de lógica difusa** – O raciocínio difuso é baseado em regras, e tem sido utilizado com sucesso nas de automação, controle, classificação de dados, analise de decisões, sistemas especialistas dentre [MAIA,2004][SILVEIRA,2005].
   O modelo de detecção de intrusão usando lógica difusa aplica as teorias da incerteza e da imprecisão para determinar uma tentativa de intrusão. Esse conceito é bem aceito, a definição de segurança em si é incerta e imprecisa, consequentemente difusa.
   Os trabalhos publicados sugerindo essa nova abordagem para aumento do grau de confiabilidade, têm sido felizes nos protótipos implementados.

2.2.4 Técnicas de resposta a ataques – contramedidas

Existem quatro classes de contramedidas que um IPS pode utilizar para bloquear um ataque [RASH,2005]. Cada classe se aplica a uma camada da pilha de protocolos, iniciando-se pela camada de enlace. Um tratamento introdutório da pilha de protocolo TCP/IP está além do assunto desta monografia.

Para este trabalho está sendo utilizado o modelo hibrido de Tanenbaum [TANENBAUM,1997], que possui cinco camadas: Física, Enlace, Rede, Transporte e Aplicação. No modelo de Tanenbaum, as camadas de seção e apresentação do modelo OSI (*Open Systems Interconnect*) foram incorporadas à camada de aplicação.

A lista a seguir ilustra as classes de contramedidas e relaciona as camadas correspondentes da pilha TCP/IP. Note que um Sistema de Resposta Ativa que não está em linha pode implementar qualquer uma das contramedidas, a não ser as da camada de aplicação. Estas últimas requerem alteração no fluxo de dados, recalculo de *checksum* e descarte de pacotes, atividades que somente um dispositivo em linha é capaz de executar. A camada física

não possui contramedida implementável, uma vez que nenhum tipo de resposta automatizada envolve a alteração física ou da característica da rede.

1. **Contramedidas da camada de enlace** – Desliga administrativamente a porta do *switch* por onde os ataques foram originados. Esse tipo de contramedida somente pode ser adotado para ataques advindos da rede local. É necessário que depois de determinado tempo, a porta retorne à sua situação inicial: seja ligada novamente, pois, uma porta de *switch* com equipamento em uso não deve ficar desligada por tempo indeterminado. As contramedidas adotadas nesta camada são extremamente críticas, uma vez que, se mal implementadas, podem desconectar toda uma rede.

2. **Contramedidas da camada de rede** – Interagem diretamente com um *firewall* externo ou um roteador para adicionar uma regra de bloqueio para todas as comunicações de determinado endereço IP ou de toda uma sub-rede. Um IPS pode executar a mesma ação de bloqueio sem a necessidade de um dispositivo externo, uma vez que pacotes originados de um endereço IP específico podem simplesmente ser bloqueados assim que o ataque é identificado. De modo semelhante às respostas da camada de enlace, definir um tempo máximo de bloqueio é importante nas contramedidas da camada de rede, uma vez que o conjunto de regras de bloqueio tanto no *firewall*, quanto no roteador, se mantidas, causarão negação do serviço que está sendo prestado.

3. **Contramedidas da camada de transporte** – Gera pacotes TCP RST para finalizar sessões TCP maliciosas, ou utiliza qualquer um dos vários pacotes informativos do ICMP, como resposta a um tráfego malicioso UDP. Note-se que ICMP é um protocolo restrito à camada de rede, mas é o método padrão para comunicação de erros UDP. Tempo máximo para validade da contramedida não é aplicável nesse caso, porque todas as ações de contramedidas são baseadas na

seção específica do ataque no caso do TCP, ou diretamente nos pacotes de ataques no caso do UDP.

4. **Contramedidas da camada de aplicação** – Altera os dados maliciosos na camada de aplicação, de forma que fiquem inofensivos antes de alcançar o alvo. Esta contramedida requer que o IPS esteja em linha, no caminho da comunicação. Qualquer cálculo de *checksum* efetuado pela camada de transporte deve ser recalculado, uma vez que houve alteração dos dados. Similar à camada de transporte, não é necessário tempo máximo de validade da contramedida, uma vez que ela é uma ação transitória. Substitui o tráfego malicioso por tráfego inofensivo, ou simplesmente efetua o descarte do pacote malicioso. Contramedidas na camada de aplicação são as mais efetivas.

2.2.5 Modelagem dos sistemas de detecção de intrusão

No final da década de 90, os ataques à sistemas computacionais ficaram cada vez mais sofisticados. Por esse motivo, fabricantes e desenvolvedores de solução de combate a intrusão, cada um a sua maneira, criavam soluções de proteção distribuídas, que atendiam e detectavam ataques de forma diferente [STANIFORD-CHEN,1998]. Contudo, essa maneira até natural de evolução representava um problema; já que, para garantir maior eficiência à detecção de intrusão, os diferentes dispositivos deveriam, de alguma forma, conversar entre si e a única forma possível disso acontecer seria se vários sistemas de detecção de intrusão trocassem informações. Contudo havia a questão: como?

Percebendo o problema, o DARPA – *Defense Advanced Research Projects Agency*–, numa tentativa de padronizar o esquema de funcionamento dos Sistemas de Detecção de Intrusão, criou o *Common Intrusion Detection Framework Working Group* (http://www.isi.edu/gost/cidf/). Esse grupo de trabalho teve como incumbência inicial desenvolver protocolos e interfaces de programação que possibilitassem aos sistemas de detecção de intrusão o

compartilhamento e a troca de informações. Como resultado principal, esse grupo definiu uma arquitetura que dividiu um Sistema de Detecção de Intrusão em componentes e um modelo em camadas, apresentando como deve funcionar a comunicação entre esses componentes [CIDFA,1999]. A figura a seguir representa graficamente este modelo.

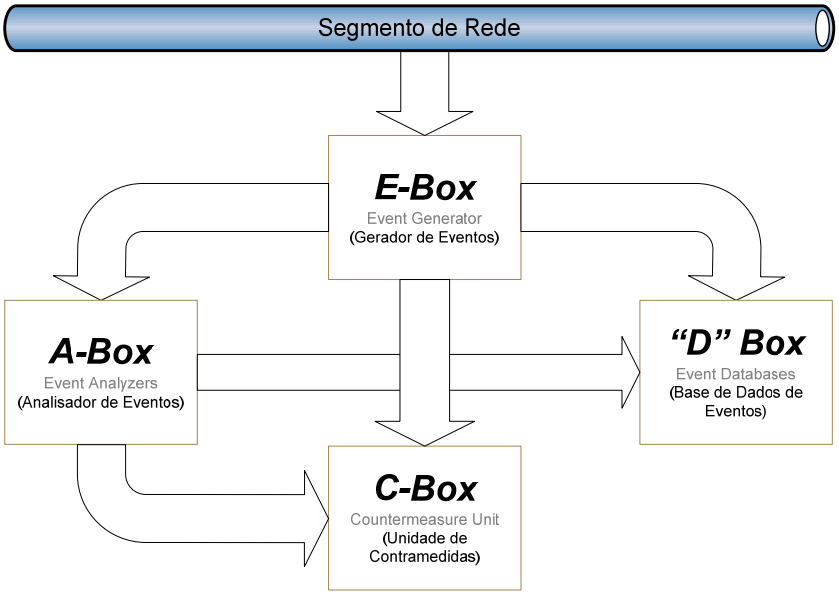


Figura 4 – Esquema de funcionamento da arquitetura CIDF e possíveis interações

A arquitetura define que um Sistema de Detecção de Intrusão é formado por componentes discretos que se comunicam por meio da passagem de mensagens, denominadas GIDO – *Generalized Intrusion Detection Objects*, que são representadas através de um formato comum, definido como CISL – *Common Intrusion Specification Language* [CISL,1999].

Os componentes são definidos como:

1. Gerador de eventos (coloquialmente "Componente E", ou ainda "Caixa E"). Sua função é detectar eventos nos dados auditados e repassar estes eventos, no formato GIDO, para os outros componentes. É chamado de sensor e em um sistema baseado em redes, que utiliza a técnica de detecção de mau uso, pode conter as assinaturas de ataques que deverão ser monitorados. Os eventos devem ser gerados assim que ocorrem, em tempo real, e o

armazenamento de eventos deve ficar sob a responsabilidade dos Bancos de Dados de Eventos – Componente D;

2. Analisador de eventos ("Componente A"). Recebe os alertas gerados por um ou mais sensores e pode realizar pesquisas no banco de dados de eventos, com o intuito de gerar estatística e correlacionar eventos. Correlação, nesse contexto, é definida por um relacionamento que é causal, complementar, paralelo ou recíproco. Eventos podem ser correlacionados pelo endereço fonte, por exemplo, a fim de identificar um possível atacante;

3. Banco de dados de eventos ("Componente D"). Armazena os eventos gerados por um ou mais sensores e é utilizado pelo analisador para correlacionar eventos;

4. Unidade de contramedidas ("Componente C"). Recebe eventos dos componentes A e E e deve tomar ações necessárias para impedir a concretização do possível ataque, como finalizar conexões e processos ou alterar permissões de arquivos e diretórios. O projeto originalmente se referiu a esta unidade como Unidade de Resposta, entretanto a maioria dos autores, para facilitar o aprendizado, refere-se a ela como Unidade de Contramedida. Essa mudança na definição se deu em virtude da evolução dos próprios sistemas de detecção, que passaram a possibilitar uma reação ativa em relação ao tráfego, por exemplo, finalizando a conexão ou ainda enviando um ICMP *host unreachable*, simulando que o equipamento foi desligado.

A ultima atualização dos trabalhos do CIDF data de setembro de 1999, o que demonstra que o projeto está parado. O IETF – *Internet Egineering Task Force*, percebendo a necessidade de dar continuidade ao estudo dos Sistemas de detecção de Intrusão, criou um grupo de trabalho cujo objetivo é definir formatos de dados e procedimentos de troca para o compartilhamento de informações de interesse em Sistemas de Detecção de Intrusão [WOOD,2006]. Esse grupo é chamado de IDWG – *Intrusion*

Detection Working Group. O trabalho do IDWG resultou na especificação de um formato para troca de mensagens (IDMEF – *Intrusion Detection Message Exchange Protocol*) e de um protocolo de comunicação para o transporte de mensagens IDMEF (IDXP – *Intrusion Detection Exchange Protocol*).

O IDWG determinou uma arquitetura para os IDS mais detalhada que o CIDF [WOOD,2006]. Os componentes especificados não são necessariamente implementados por todos os Sistemas de Detecção de Intrusão. Entretanto, podem ser implementados em um único módulo ou distribuídos em múltiplos módulos. A figura a seguir apresenta graficamente estes componentes.

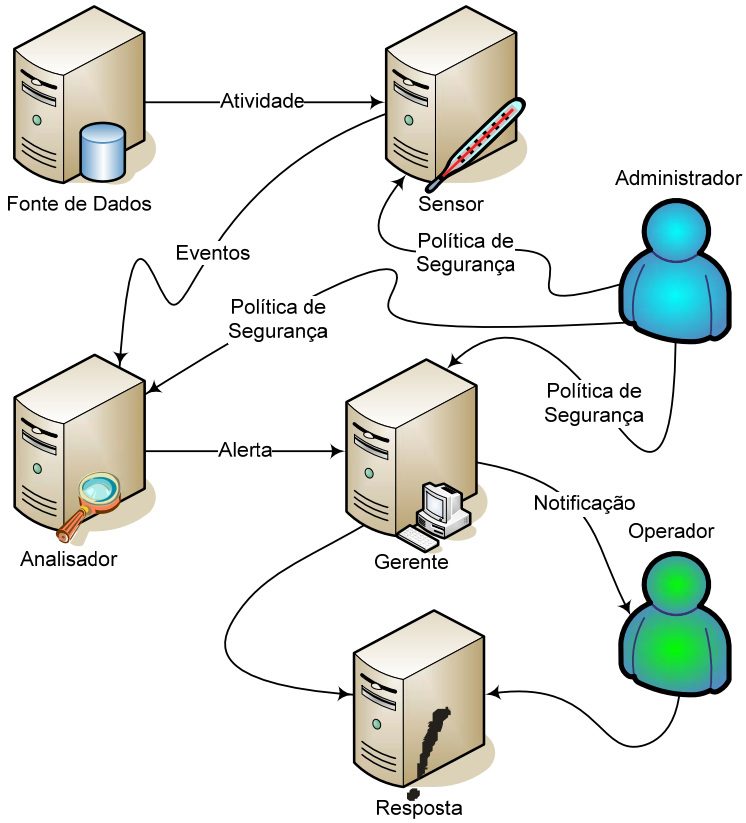


Figura 5 – Esquema de componentes do IDWG para IDS's

Segue explicação de cada elemento da figura 5:

- Atividade. Elementos ou ocorrências da Fonte de Dados que são identificados pelo Sensor ou Analisador como de interesse do Operador.

- Alerta. Uma mensagem do Analisador para o Gerente que um evento de interesse, ou seja, um evento definido pela política foi detectado;

- Analisador. Componente ou processo que analisa os dados coletados pelo sensor, ou pelos sensores, procurando sinais de atividade suspeita ou por eventos de interesse do Administrador. Em muitos sistemas, o Sensor e o Analisador são implementados no mesmo dispositivo físico.

- Evento. Ocorrência na Fonte de Dados detectada pelo Sensor e que pode resultar em um Alerta transmitido ao Gerente.

- Fonte de Dados. Dados brutos a serem auditados. Exemplo comum de fonte de dados é o tráfego em um segmento.

- Gerente. Componente ou processo pelo qual o Administrador gerencia os vários componentes do sistema. Funções de gerenciamento incluem a configuração de um ou mais sensores, gerenciamento de notificação de eventos e geração de relatórios;

- Notificação. O método pelo qual o Gerente informa o Operador da ocorrência de um Alerta e do Evento que gerou o Alerta. Pode ser um e-mail, uma entrada no *log*, um *trap* SNMP, um alerta sonoro, um alerta visual, ou até mesmo a realização de uma conexão *socket*.

- Operador. A pessoa que é o usuário primário do Gerente e monitora a saída do sistema e inicia ou recomenda ações de resposta;

- Resposta. Ações tomadas em resposta a um evento. Podem ser automáticas ou iniciadas pelo Operador;

- Sensor. Componente que coleta dados da Fonte de Dados e é configurado para repassar eventos ao Analisador.

- Assinatura. Uma regra utilizada pelo Analisador para identificar atividades de interesse do Administrador. Assinaturas representam

um dos mecanismos pelo qual o Sistema detecta intrusões, mas não necessariamente o único.

- Política de Segurança. As sentenças predefinidas e documentadas que identificam quais atividades são permitidas na rede ou em *hosts* de uma organização.

- Política: Ações que deverão ser analisadas ou descartadas pelo Sensor ou Analisador.

O IDWG é o grupo internacional de definições de padrões para sistemas contra intrusos. Concluiu seu trabalho gerando propostas de novos protocolos em março de 2006. Essas especificações estão no formato *Internet-Draft*, aguardando a aprovação do IETF para se tornarem RFC – *Request for Comments*, para que então sejam submetidos ao processo de aprovação como padrões.

2.2.6 Modelagem dos sistemas de prevenção de intrusão

Os IPS herdaram todos os modelos de funcionamento dos IDS, sendo impossível dissociar um do outro. Por seu esquema de funcionamento ser melhor, evitando o ataque, o IPS precisa agregar várias funções em um mesmo equipamento. A figura a seguir é uma adaptação do modelo do IDWG para IPS.

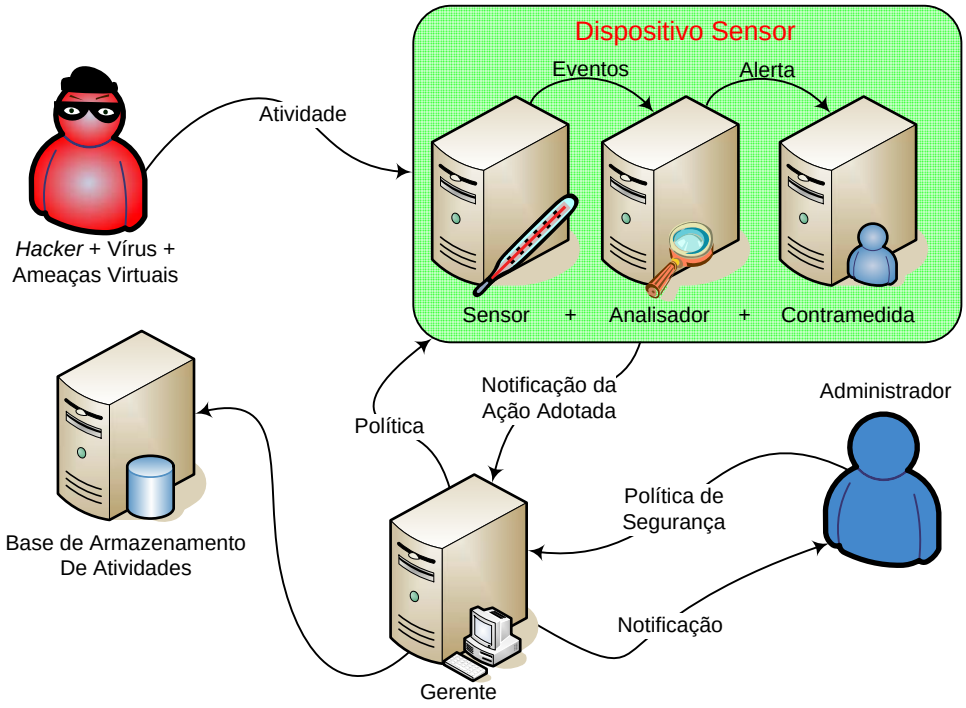


Figura 6 – Esquema de componentes para IPS

Segue explicação de cada elemento da figura a cima:

- *Hacker*, vírus e ameaças virtuais: Elementos geradores de atividades que visam invadir, danificar ou degradar a *performance* do ambiente de rede.

- Atividade: Elementos ou ocorrências oriundos da rede que são identificados pelo Sensor segundo política definido pelo Administrador;

- Dispositivo Sensor: Dispositivo de *hardware* que agrega em um mesmo equipamento as funções de Sensor, Analisador e Dispositivo de Contramedida.

- Sensor: Componente de software responsável por fazer a primeira análise, procura ataques pré-definidos pela política, efetua a análise rápida, normalmente procura por ataques de *pattern matching*.

- Analisador: Componente de *software* responsável pela segunda análise, procura por ataques desconhecidos por meio de análise de

comportamento. Consome mais recursos de hardware e procura comportamentos que fogem do padrão.

- Dispositivo de Contramedida: Responsável pela ação a ser adotada quando um ataque é identificado. Nas soluções de IPS esse pedaço de *software* deve estar no mesmo *hardware* que identifica o ataque. Ele precisa descartar o pacote e recalcular o *checksum* dos próximos pacotes para que não haja perda da conexão estabelecida.

- Notificação da Ação Adotada: Informa ao equipamento de gerência do ataque e da ação adotada.

3 ANÁLISE FORENSE

3.1 INTRODUÇÃO

A ciência forense, ou simplesmente forense, pode ser definida como a aplicação de várias ciências para responder perguntas de interesse do sistema legal, tendo estas, normalmente, relação com um crime ou com uma ação civil [WIKIFOR,2006].

A ciência forense está intimamente ligada à criminalística, que é a utilização de ciências variadas para responder a perguntas que se relacionam com exame e comparação de evidências criminais, sejam elas biológicas, de impressão – tal como impressões digitais, pegadas, e marcas de pneu –, de substâncias controladas, de armas de fogo ou qualquer outro tipo de evidência em investigações criminais.

Existem inúmeras ciências forenses. A Patologia Forense, por exemplo, efetua o estudo do corpo humano para determinar a causa ou a maneira da morte. Já a Odontologia Forense estuda a unicidade da arcada dentária. A Toxicologia Forense, por sua vez, é o estudo dos efeitos das drogas e venenos no corpo humano. Engenharia Forense é o estudo das causas de falhas em dispositivos ou estruturas. Psicologia e Psiquiatria Forense estudam, ambas, os aspectos legais do comportamento humano. Antropologia Forense é a aplicação dos princípios e métodos da antropologia física, em um determinado ambiente, para recuperação e identificação de restos de esqueletos humanos. Entomologia Forense trata-se do estudo de insetos dentro, fora e ao redor dos humanos para auxiliar na determinação da hora ou localização da morte.

O primeiro uso da ciência forense de que se tem conhecimento foi a prova feita por Arquimedes de que uma coroa não era de ouro, como o ourives que a forjou declarava. Arquimedes provou a fraude verificando a densidade da peça. O famoso termo “Eureka” vem desse episódio [TERRA,2006]. O

primeiro relato do uso de impressões digitais para determinar identidades data do século VII. Segundo Soleiman, um comerciante árabe, as impressões digitais de devedores eram anexadas a contas, que ficavam com os credores. Essas contas eram legalmente reconhecidas como prova da validade do débito [WIKIFOR,2006].

O primeiro registro do uso da entomologia para apurar crimes está no livro *Xi Yuan Ji Lu* (Coleção de Casos de Injustiça Corrigida) escrito na China em 1248 por Song Ci. Em um desses casos, o autor conta sobre um assassinato executado com uma foice, que foi resolvido por um investigador que instruiu que todos levassem suas foices a um mesmo local. Moscas, atraídas pelo cheiro de sangue, rodearam apenas uma das foices. Diante do ocorrido o assassino confessou o crime. O livro relata também sobre como distinguir o afogamento (água nos pulmões) do estrangulamento (cartilagem quebrada da garganta).

Durante o século XVI, graças à ação dos médicos ao manterem registros de informações sobre causa e maneira da morte, universidades e estudiosos da época puderam fazer vários estudos e com isso contribuíram para o avanço da medicina forense. Em 1775, Carl Wilhelm Scheele, um químico sueco, desenvolveu um método para detectar a presença de arsênico em grande quantidade em cadáveres. Desde então a ciência forense não parou de crescer, agregando cada vez mais novos estudos e ciências auxiliares na descoberta de crimes.

Diversos campos do conhecimento humano podem estar relacionados com questões da ciência forense, como a medicina, por exemplo, quando se trata de determinar a causa de uma morte; ou a química para detectar resíduos de determinados compostos utilizados em um crime.

Este trabalho ficará limitado à Ciência Forense Digital, ou Forense Computacional. Ela pode ser definida como o processo de investigação de dispositivos de armazenamento ou processamento de dados – computador doméstico, *laptop*, servidor, estação de trabalho, mídia removível etc. –, para

determinar se o equipamento foi usado de forma ilegal, não-autorizada, ou para atividades suspeitas. Esse processo também inclui o monitoramento da rede com o mesmo propósito [WIKICOMPFOR,2006].

3.2 A FORENSE COMPUTACIONAL

Forense Computacional é a aplicação de métodos e procedimentos científicos em meio digital com o intuito de determinar informações factuais para apresentação e utilização no sistema jurídico [WIKICOMPFOR,2006]. Esse processo usualmente envolve a investigação de sistemas computacionais para identificar e determinar a utilização passada ou presente desses sistemas, em atividade ilegal ou não autorizada. Na maioria das vezes, os peritos digitais investigam os dispositivos de armazenamento – mesmo os danificados, como por exemplo, discos rígidos, CD-ROM´s, fitas DAT ou qualquer outro dispositivo de armazenamento.

Como regra geral, a análise forense computacional deve ser executada de forma a manter um padrão técnico admissível em uma corte judicial.

A forense computacional é subdividida em várias especialidades: análise de arquivos, análise de sistema de arquivos, análise de informações criptografadas, verificação de dispositivos de *hardware*, recuperação de informações em dispositivos danificados, esteganografia, análise de metadados e forense de rede. O escopo desse trabalho limitar-se-á à forense de rede.

3.2.1 Forense de rede

Pode ser definido como o processo de captura, gravação e análise de eventos de redes com o intuito de descobrir a fonte de ataques ou de incidentes de segurança [FORWIKI,2006][WHATIS,2006]. De acordo com Simson Garfinkel, os sistemas de forense de rede podem ser classificados em dois tipos:

- Sistemas de Captura Bruta (*Catch-it-as-you-can Systems*) – Todo tráfego que passa pelo dispositivo de captura é armazenado e analisado subseqüentemente em modo *batch*. Esse tipo de sistema requer grande espaço em dispositivo de armazenamento, normalmente envolvendo dispositivos RAID.

- Sistema de Análise em Tempo Real (*Stop, look and listen Systems*) – O pacote é analisado em tempo real na memória, e somente informação relevante é armazenada para análise futura. Esse tipo de sistema necessita de alta capacidade de processamento para manter a análise em tempo real sem perda de informação.

Ambos os dispositivos precisam de certa capacidade de armazenamento e a necessidade ocasional da exclusão de dados antigos para dar espaço a dados novos. Tanto programas de código aberto (*TCPDump*, *Windump*) como programas proprietários (*Sniffer*) podem ser utilizados para captura de dados e ferramenta de suporte à análise forense.

A preocupação comum acerca dos sistemas de captura bruta diz respeito à questão da privacidade, uma vez que toda a informação do pacote é capturada (incluído o campo *data*, ou seja, os dados do usuário).

Os Estados Unidos possuem legislação específica para proteger a privacidade dos usuários de provedores de acesso a Internet e operadoras de telefonia, proibindo por meio do Ato para Privacidade das Comunicações Eletrônicas (ECPA – *Eletronic Communications Privacy Act*), a captura ou a divulgação de conteúdo eletrônico interceptado, exceto com autorização expressa do usuário ou por determinação judicial. A única normativa legal que existe no Brasil – e que pode ser considerada uma norma embrionária sobre privacidade –, foi introduzida na Legislação Brasileira por meio do artigo 10 da Lei 9.296 de 24 de julho de 1996. Esse artigo prega:

> *Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.*

Um exemplo controverso de ferramenta de forense de rede é o *Carnivore* do FBI. [SHOWSTUFF,2006] Apesar da proibição expressa pelo ECPA, o *Carnivore* é a ferramenta desenvolvida e utilizada pelo FBI com o intuito de policiar ações terroristas, de espionagem, fraudes e pornografia infantil. Essa ferramenta, além de interceptar e analisar tráfego, gera informações consolidadas para uso em corte judicial americana. Ela é considerada controversa porque o FBI se recusa a tornar público seu código-fonte.

Produtos para forense de rede são conhecidos também como Ferramentas de Análise Forense de Rede.

3.2.2 Captura de informações para forense de rede

A execução de uma análise forense de rede é executada utilizando como fonte de informação principalmente dois elementos: *logs* e a cópia do tráfego de rede capturado previamente.

O processo de captura dessas informações é executado por diversos dispositivos na rede. Pode envolver a análise prévia dos dados antes de se efetuar um lançamento de registro [JONES,2006]. A captura e armazenamento do tráfego de rede estão associados a dispositivos específicos para forense de rede, uma vez que esse tipo de ação consome recursos tanto de máquina quanto de rede. Já os *logs* são registros de eventos que podem ocorrer nas diversas camadas de rede, ou nos vários dispositivos da rede onde serviços estão instalados.

As possíveis fontes de dados para a análise forense de rede foram classificadas em quatro grupos:

- **Registros de sessão** – São registros com o resumo das trocas de informações de uma comunicação. Podem ser gerados por qualquer dispositivo de rede que receba, faça ou monitore o tráfego na camada de rede e transporte, respectivamente camadas 3 e 4 do modelo OSI. Exemplo: *firewall*, servidor *web*, servidor de e-mail etc.

- **Registro de dados estatísticos** – São registros relativos à quantidade de dados e protocolos utilizados na transmissão. Fornece poucas informações para o perito sobre as quebras de segurança propriamente ditas. No campo prático, ajudam o perito a se informar sobre protocolos e portas não-usuais que estão sendo utilizadas, bem como possíveis canais de espionagem.

- **Registro de alertas** – São registros de alertas gerados para predeterminados itens de interesses, normalmente por dispositivos especialistas tais como os sistemas de detecção/prevenção de intrusão. A usabilidade das informações destes arquivos é diretamente proporcional a qualidade da configuração do dispositivo, se o IDS/IPS não estiver configurado para perceber determinado tráfego, alertas relativos a esse tráfego não serão registrados.

- **Cópia do tráfego** – É realizado por dispositivos dedicados para forense de rede. Seu funcionamento consiste no armazenamento de todo bit da transação, para caso seja necessário, o investigador tenha uma fonte de dados com a cópia do tráfego para executar seu trabalho. A lógica desta solução é que armazenado todo o tráfego, as informações relativas ao ataque também estarão guardadas. É uma solução cara, que exige mídias com alta capacidade para armazenamento.

3.3 O PERITO FORENSE

São atribuições dos especialistas em análise forense computacional identificar suspeitos e fontes de evidências, obter e preservar evidências digitais, analisar essas evidências e apresentar um relatório com as conclusões da análise. Isto deve ser feito utilizando procedimentos padronizados e aceitos pela comunidade científica, para que os resultados obtidos durante uma análise sejam passíveis de reprodução, bem como as provas produzidas sejam aceitas em um processo judicial [OLIVEIRA,2002].

Marcelo Reis e Paulo Lício, no trabalho “Forense Computacional: Procedimentos e Padrões” [REIS,2002], propuseram um modelo de padronização para procedimentos de exames periciais em sistemas computacionais.

A figura a seguir representa graficamente o modelo hierárquico proposto por eles.

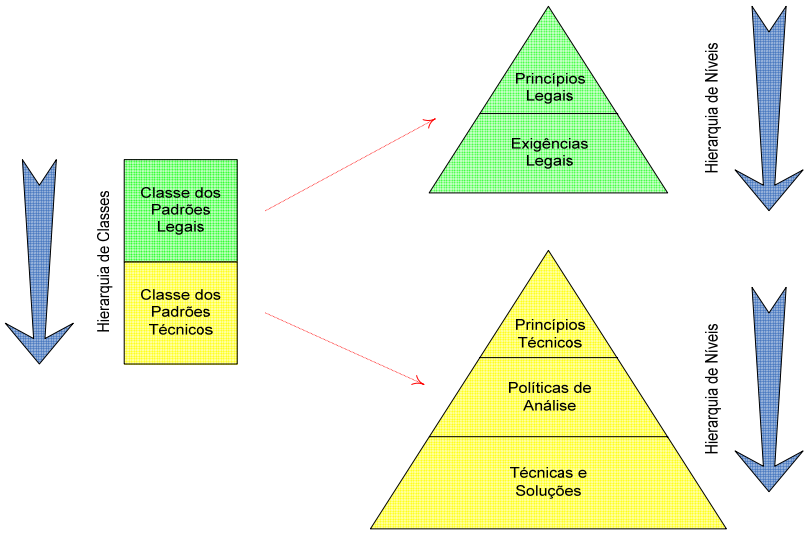


Figura 7 – Modelo de Padronização para exames periciais digitais

O modelo, dividido em duas classes, ilustra os requisitos práticos e condutas a serem adotadas pelos peritos criminais digitais, tendo como norteador as formalidades e enquadramentos judiciais que permitam a utilização das evidências digitais por jurisdições com diferentes legislações.

A divisão em classes permite ao perito executar suas ações de forma independente dos quesitos legais. De uma maneira geral, as políticas para execução de um exame pericial seguem o esboço abaixo, podendo variar de acordo com a particularidade do sistema a ser examinado e do tipo de análise.

Passo 0: Determinar a melhor abordagem para o exame, identificando todas as atividades a serem executadas;

Passo 1: Preparar o sistema de análise, provisionando a melhor

configuração de *hardware* e *software*. O material deverá ser testado e esterilizado antes da realização dos exames. O ideal é recriar o ambiente da maneira mais próxima ao da ocorrência do fato;

Passo 2: Estabelecer a condição ideal do sistema computacional a ser examinado, de modo a preservar o máximo de vestígios possíveis e proteger os dados e sistemas não comprometidos. Todo o procedimento deve ser minuciosamente documentado;

Passo 3: Efetuar cópia das informações relevantes, na ordem de volatilidade das mesmas. A cópia deve conter toda a informação e estas deverão ser autenticadas;

Passo 4: Buscar indícios analisando cada informação separadamente, em seguida, de forma correlata;

Passo 5: Estabelecer, se possível, as relações entre os indícios encontrados (indícios digitais ou não);

Passo 6: Emitir o laudo pericial com o parecer final, reunindo todas as informações resultantes do exame.

De forma resumida, as ações podem ser agrupadas em quatro grupos de atividades:

1 – Identificar as fontes de documentação ou outra evidência digital.
2 – Preservar a evidência.
3 – Analisar a evidência.
4 – Apresentar os fatos encontrados.

3.4 A PROVA DIGITAL

O mundo do perito digital gira em torno da evidência. O termo “evidência” refere-se a toda e qualquer informação capaz de determinar a ocorrência de um crime ou que provê algum elo entre o crime e vítima ou entre o crime e o

criminoso [CASEY,2004]. No contexto eletrônico, essa evidência é digital. Apesar de a legislação brasileira definir apenas o conceito de “prova”, o termo evidência, na literatura forense é largamente utilizado, devendo ser entendido como prova material no caso da evidência física e prova documental no caso da evidência lógica.

A evidência digital possui algumas características próprias. Primeiramente ela permite duplicação perfeita, possibilitando a preservação da evidência original durante a análise. É relativamente fácil determinar se uma evidência digital foi modificada. Por outro lado, ela é extremamente volátil, podendo ser facilmente alterada durante o processo de análise.

A busca de provas em um sistema computacional constitui-se de uma varredura minuciosa nas informações que nele residem, sejam dados em arquivos ou em memória, “apagados” ou não, criptografados ou possivelmente danificados.

Quando se trata de forense em dispositivos comprometidos, a evidência pode ser física, uma vez que a análise inicia-se pelo estudo de um dispositivo de armazenamento físico, tal como o disco rígido. Entretanto quando trata-se de forense de rede a análise toma forma essencialmente lógica.

3.4.1 Cadeia de custódia ou corrente de custódia

A cadeia de custódia é um conceito legal que se aplica ao uso e manuseio da prova para que seja mantida a sua integridade [WIKICHAIN,2006] [FREITAS,2004][TOXLAB,2006].

A cadeia de custódia se refere também à documentação produzida sobre a apreensão, custódia, controle, transferência, análise e disposição de uma prova, seja ela material ou documental, no caso deste projeto, física ou eletrônica. Ou seja, é o processo utilizado para manter e documentar cronologicamente o histórico de uma prova.

O papel da prova numa corte é convencer o juiz da culpabilidade ou inocência de um réu, portanto toda prova deve ser manuseada de forma extremamente cuidadosa, a fim de evitar futuras alegações de adulteração. Tal alegação, se comprovada, pode comprometer o processo de condenação e arruinar um caso.

Estabelecer a cadeia de custódia é essencialmente importante quando a prova consiste em um bem de valor. Na prática a cadeia de custódia é aplicada freqüentemente quando da apreensão de drogas ilícitas. Uma pessoa ou departamento precisa ter a custódia física da prova. Na prática isso significa que o policial ou detetive deve coletar a prova, documentar todo o procedimento e entregar a prova para armazenamento seguro. Estas transações – e todas as transações subseqüentes entre a coleta da prova e apresentação em corte – devem ser completamente documentadas, de forma cronológica, a fim de suportar questionamentos legais quanto à autenticidade desta prova. A documentação deve sempre incluir as circunstâncias sob as quais a prova é recolhida, a listagem detalhada dos indivíduos e o período que tiveram o material apreendido sobre seu poder. Entre as informações relevantes que merecem ser documentadas estão data e hora da ação, a quem pertencia o material ou quem forneceu, local da apreensão, descrição completa do material, de quem as provas foram recebidas, a quem foram entregues e quaisquer outras informações peculiares ao caso.

4 MODELO PARA CAPTURA E ARMAZENAMENTO SEGURO E CONFIÁVEL DE TRÁFEGO

A idéia da associação de um sistema de detecção de intrusão e a utilização de seus *logs* para análise forense não é nova, entretanto, não existe modelo formal definido nem de quais informações devam ser armazenadas, nem tão pouco de como armazená-las.

Inúmeras estratégias poderiam ser adotadas ao se armazenar informações para o perito, entretanto a mais vantajosa, a que dá o maior número de elementos é armazenar o tráfego, o pacote de informação e não somente informações sobre o ataque, como normalmente os IDS/IPS fazem.

Este modelo aborda a questão do que deve ser armazenado, como se armazenar essa informação, e como dar validade ao processo de captura e armazenamento desse tráfego.

4.1 SOLUÇÕES COMERCIAIS

Para esboçar qualquer tentativa de definir qual tráfego é relevante para que um Sistema de Prevenção faça captura, é necessária uma análise abrangente dos fatores ligados a invasão. É preciso observar as mentes criminosas que estariam por trás de invasões a sistemas. Hoje a tecnologia disponível transformou o computador e a Internet em meios viáveis de “ganhos fáceis”. Sem se fazer fisicamente presente, um criminoso pode agir e fazer suas investidas. O atacante ganhou maior liberdade e atua com certa sensação de segurança e, mesmo que na maioria das investidas o indivíduo não logre sucesso, existe a possibilidade real que após muitas tentativas um cyberterrorista consiga atingir o objetivo.

É perfeitamente lógico então, considerar que, na maior parte das vezes, um ataque “bem sucedido” é precedido de várias tentativas sem êxito.

Se essas tentativas forem documentadas, essa documentação pode servir

como prova em um processo criminal. Esse processo de captura e armazenamento de informações é o primeiro passo para a forense de rede computacional.

Já existem várias soluções no mercado que armazenam todo o tráfego que passa pelo dispositivo de captura, mas a primeira solução comercial lançada foi proposta pela *Sniffer Technologies*, empresa americana, à época uma divisão da *Network Associates Inc.* A solução simples e eficiente foi batizada de *Infinistream,* um dispositivo de rede com capacidade de armazenamento que varia de 300 *gigabytes* a 4 *terabytes* e armazena todo tráfego.

Em seu funcionamento, uma vez alcançada a capacidade máxima de armazenamento do dispositivo, o tráfego “mais antigo” é descartado, criando espaço para o tráfego mais novo; o que resulta na quantidade do tráfego ser inversamente proporcional ao tempo de armazenamento.

A primeira versão do *Infinistream* era especializada para análise forense; remontava o fluxo do tráfego e as ações do atacante, mostrando ao perito digital, por meio de um simulador, a tela do computador do agressor com registro das ações tomadas ao longo do tempo. Nesta versão o software trabalhava com SMTP, POP, IMAP4, HTTP, FTP, IRC e *VoIP*, o que significa dizer que ele estava preparado para registrar e armazenar ataques dos aplicativos mais utilizados na Internet.

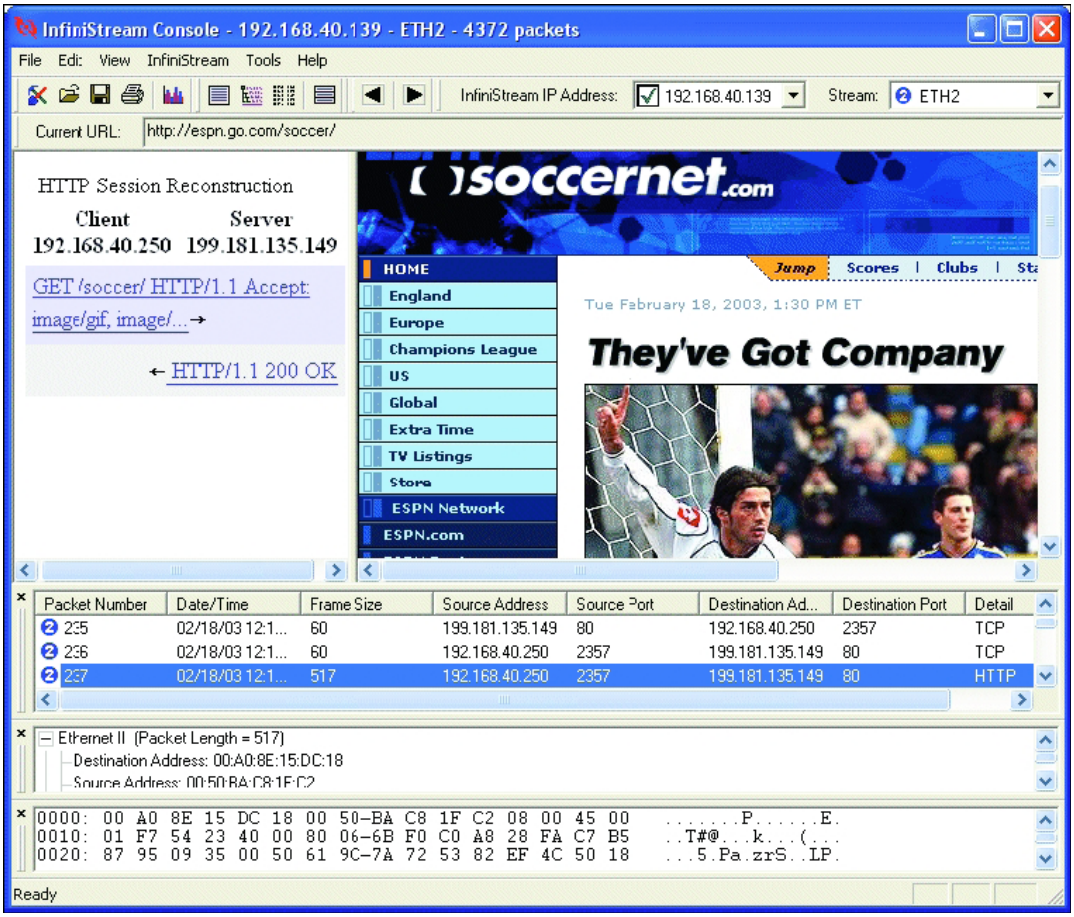


Figura 8 – *Infinistream* reconstruindo uma sessão HTTP

É necessário destacar que existem ataques efetuados pela Internet, que utilizam como principal ferramenta para acesso remoto uma sessão Telnet ou SSH e o *Infinistream* não armazenava tal tráfego. Surge então a questão acerca da utilidade do uso de uma ferramenta que não armazena os principais protocolos utilizados em ataques. Vale ainda salientar que o protocolo SSH é um protocolo para acesso remoto seguro (*Secure Shell*), ou seja, é seguro por utilizar comunicação ponto a ponto criptografada, de modo que ainda que o *Infinistream* armazenasse esse tipo de tráfego, não adiantaria ao perito ter acesso ao tráfego criptografado. Decifrar consumiria tempo e não preveniria, posto que o ataque já teria ocorrido. A análise desse tráfego somente poderia ser útil para determinar onde ocorrera a falha e corrigir uma vulnerabilidade qualquer, que, porventura tenha possibilitado o ataque.

Entretanto, uma ação dessa natureza precisa ser feita no menor tempo

possível, possibilidade esta que no caso em questão ficaria comprometida pela necessidade de descriptografia e análise.

Em virtude desses fatores, o mercado não recebeu bem a solução criada pela *Sniffer Technologies*. Posteriormente a companhia foi vendida e o desenvolvimento do *Infinistream* tomou outro rumo. Continua sendo uma ferramenta que armazena tráfego, entretanto, o foco maior é para análise de desempenho da rede. A até então ferramenta de remontagem do fluxo perdeu lugar para o analisador de protocolo *Sniffer*. A ferramenta hoje ainda pode ser utilizada para análise forense, mas não com a mesma facilidade de análise de outrora.

Existem no mercado outras soluções para captura e análise forense de rede, cada qual com suas próprias características, mas, todos muito funcionais quanto à forense de rede. Por exemplo: *NetIntercept* (http://www.sandstorm.net/products/netintercept/), *NetDetector 2005* (www.niksun.com), *NetWitness* (www.forensicsexplorers.com) e o *eTrust™ Network Forensics r8* (http://www3.ca.com/solutions/Product.aspx?ID=4856).

O destaque se dá para o *eTrust*. A solução desenvolvida e comercializada pela CA – *Computer Associates* é a única hoje do mercado que trabalha com a tecnologia n-grama. Essa é uma tecnologia de mineração de dados, específica para correlacionamento de conteúdo em largas bases de dados por permitir, em um tempo relativamente menor do que o convencional, a busca de informações. Ele funciona procurando seqüências de cadeia de caracteres de comprimento “n” tiradas de um determinado documento (e-mail, página *web* etc.), utilizando como entrada o tráfego, ou um dado informado pelo analista.

Voltando a solução *Infinistream*, um *appliance* com maior capacidade de armazenamento, 4 *terabytes*, armazenando o tráfego de um *link* de 2mbits/s com taxa de ocupação média de 40%, conseguiria armazenar informação de aproximadamente 1 ano e 5 meses. Ou mais precisamente 1 ano, 4 meses, 29 dias, 47 minutos e 45 segundos.

É importante destacar que 4 *terabytes* com um ano de informação já representa muito trabalho de pesquisa para um perito digital, pode-se então imaginar o que significaria procurar ataques em uma base com 4 *tera*. Mesmo com o uso do n-grama, busca em uma base deste tamanho pode levar dias.

Vem à tona uma questão: se o período de um ano representa um grande volume de informação, qual seria então um período de tempo razoável, o tempo ideal?

A literatura especializada disponível preceitua que esse tempo deve ser proporcional à criticidade das informações para o negócio. Ou seja, faz-se necessária uma análise para avaliação e determinação do que é necessário investir, bem como a verificação do que representa um ônus maior, se o fator armazenamento ou a própria informação. Seguindo esse raciocínio, é necessário definir qual seria a criticidade de armazenamento de um tráfego passado.

Sob determinado ponto de vista, a resposta seria: nenhum, visto que o ataque que eventualmente ocorrer é passado e essas informações "passadas", na pior das hipóteses, iriam ajudar o administrador a corrigir um problema e, talvez, numa visão muito otimista, submeter o atacante às penalidades cabíveis.

Sob essa ótica, o tráfego passado deixa de ter foco no negócio propriamente dito e passa para uma visão mais abrangente, focada no ambiente, na manutenção do todo. Considere a mudança de estratégia: em vez de armazenar tudo, armazenar parcialmente.

Considerando a pilha de protocolos da Internet, é possível verificar que as comunicações se dão basicamente em duas linhas, as comunicações orientadas à conexão e as não-orientadas à conexão, respectivamente o TCP – *Transmission Control Protocol* e o UDP – *User Datagram Protocol*. O primeiro garante que o pacote de informações que saiu vai chegar – é

utilizado quando é necessário confiabilidade; e o segundo é um protocolo leve e funciona para troca rápida de informações ou quando não é necessário confiabilidade.

Um exemplo de que a confiabilidade na transmissão é desnecessária seria um *broadcast* televisivo pela Internet. Se um pacote que contém uma fração de segundo de voz não chegou, isso não importa, uma vez que nesse momento já está havendo tráfego de informação nova e a frase em questão fica sem a fração de segundo.

Sistemas de Prevenção de Intrusão, ao realizarem análise em uma camada de aplicação, conseguem detectar ataques no meio de um fluxo de comunicação, tanto TCP quando UDP. Um fluxo de comunicação pode ser definido como um conjunto de pacotes com mesma origem e mesmo destino, com números seqüenciais crescentes na identificação dos pacotes.

4.2 O QUE ARMAZENAR

Esse projeto propõe que se as tentativas de invasão forem documentadas, esta documentação pode servir como prova em um processo criminal. Detalhando-se o que está sendo dito, a documentação dessas tentativas poderia ser feita de inúmeras formas, entretanto a mais vantajosa, a que dá o maior número de elementos ao perito é armazenar o tráfego, e não somente informações sobre o ataque.

Esse armazenamento obrigatoriamente deverá ser feito através da captura do tráfego da rede. Desta forma o perito terá mais informações para executar sua tarefa de análise. Essa captura pode ser feita de quatro formas principais.

4.2.1 Captura do fluxo dos pacotes

Uma abordagem interessante para economizar espaço em disco e facilitar a busca de informações, seria o armazenamento somente dos fluxos de

comunicação contendo os ataques, o fluxo TCP ou UDP. Isso funcionaria como um armazenamento de fluxos completos de comunicação, nos quais após a detecção de um ataque, todo fluxo em que o pacote "agressor" fosse identificado ficaria armazenado. Essa solução reduziria muito o crescimento do banco, bem como permitiria guardar informações por um tempo maior do que o possível se todo tráfego fosse armazenado.

A maior dificuldade dessa abordagem estaria na maneira empregada para efetuar o armazenamento desse tráfego; seria necessário usar alguma técnica para o controle do descarte. A sugestão seria de que, a principio, todo estabelecimento de uma nova conexão e os pacotes seguintes fossem armazenados. Caso não fosse detectado ataque, esse tráfego armazenado seria excluído do banco de dados.

Uma outra camada de controle deveria ser empregada para manutenção do banco. Algoritmos de limpeza e manutenção das tabelas do banco deveriam ser utilizados com certa periodicidade para que fossem mantidas a consistência e confiabilidade desta base de dados.

4.2.2 Captura limitada por tempo

Uma outra abordagem pode ser adotada na captura do tráfego da rede: a limitação por tempo. O sistema de prevenção, quando da detecção de um ataque capturaria os pacotes por um tempo predeterminado, capturando o pacote que gerou o alerta e os pacotes subseqüentes por um tempo predeterminado. Isso reduziria de forma significativa o uso da capacidade de armazenamento do dispositivo.

Entretanto, essa abordagem também apresenta um problema. No caso de um atacante efetuar um segundo ataque dentro do período de captura do primeiro, qual seria o comportamento adotado do processo de captura? Armazenagem dos dois ataques?

Para resolver o problema, um algoritmo dotado de inteligência forense

poderia tomar forma para realizar as associações dos ataques, agrupando-as por um "suposto" atacante, agregando as tentativas de maneira inteligível, por fluxo.

4.2.3 Captura limitada por número de pacotes

Da mesma forma que a abordagem de limitação por tempo, a abordagem de limitação por número de pacotes pode ser viável. Apresenta, contudo, o mesmo problema da abordagem já sugerida no tocante a captura de ataques de uma mesma origem num curto período de tempo.

A vantagem da limitação por pacotes sobre a limitação por tempo seria referente à estrutura com que ficaria o banco de dados; os dados armazenados no banco com limitação por pacote os ataques armazenados possuiriam aproximadamente a mesma quantidade de dados, facilitando assim a manutenção e administração desse banco.

4.2.4 Captura do pacote identificado como agressor

A abordagem de captura por pacote, como pode ser observado, é a mais simples. Consiste na captura exclusiva do pacote que gerou o alerta. O ponto a ser destacado é que, por ser uma abordagem simplista, traria informações insuficientes ao analista forense, uma vez que a identificação do pacote atacante certamente estaria associada a uma assinatura de ataque conhecido ou um comportamento agressivo documentado.

4.3 A QUESTÃO LEGAL

A proposta inicial desse projeto é esboçar uma solução que dê ao analista forense provas digitais que possam ser utilizadas em um tribunal. Entretanto a prova digital de tráfego de rede, em cerca de 90% dos casos de investigação policial, é composta por *logs. E logs* podem ser facilmente adulterados. Garantir autenticidade dos *logs* é um dos problemas a ser tratado.

Antes de tudo é necessário encontrar uma técnica para dar validade a esses arquivos, e essa técnica precisa estar amparada por alguma norma legal. Na vida real, quando um perito efetua uma análise forense, ele efetua essa validação dos *logs*, transformando-os em prova documental, afinal na maioria dos casos ele é um agente policial, representando o Estado na solução de crimes. Mas que técnica fundamentada em lei poderia ser utilizada para validar os *logs*?

A questão da validade dos *logs*, gira em torno da "prova". O conceito de "prova" é juridicamente definido como qualquer informação lícita com valor comprobatório, seja para confirmar ou rejeitar determinada hipótese. Ou seja, uma prova é qualquer instrumento de que se serve o magistrado para o conhecimento dos fatos, seja documental, testemunhal ou pericial [MARINONI,2004].

O Código Processual Penal (CPP), em seu art. 158 determina que, quando a infração deixar vestígios, será indispensável o exame de corpo de delito; ou seja, é essencial o recolhimento de provas que comprovem a ocorrência do crime por intermédio de perícia técnica [LIRA,2005].

A proposta seria automatizar o processo de autenticação e validação dos *logs*. Para que estas ações sejam validadas, retirando a obrigatoriedade da presença do agente policial dessa parte inicial do processo, é necessário que todo o procedimento de coleta esteja em conformidade com a lei.

Para dar legalidade a esse processo existem algumas estratégias que poderiam ser adotadas: a primeira, seria utilizar uma lei específica, proposta e aprovada no Congresso Nacional. No Brasil, até agora, as tentativas para definição e aprovação de sanções contra os chamados crimes de informática não obtiveram sucesso, visto que a maior parte permanece tramitando num ir e vir nas casas do Congresso Nacional. Exemplo disto são os projetos de lei n.^{os} 1713/96, 84/1999, 3016/2000.

Uma outra estratégia seria utilizar a base legal regida por jurisprudências.

Jurisprudências são séries contínuas de decisões dos diversos Tribunais, no mesmo sentido, em que as leis são interpretadas e aplicadas [FELIPPE,2002]. Essas decisões conforme a Emenda Constitucional 45 deveriam servir de base para compor uma súmula vinculante.

O preceito da súmula vinculante prega que seu teor deve obrigatoriamente ser seguido para sentenças e decisões em julgamentos futuros. Isto é também conhecido no meio jurídico como efeito vinculante. Todavia, a matéria ainda é um assunto controverso. Alguns argumentam que a adoção desta súmula vinculante, retiraria do juiz a liberdade e imparcialidade do julgamento, obrigando-o a seguir uma sentença definida outrora.

A terceira e última estratégia seria utilizar algum outro instrumento legal – Resolução, Medida-Provisória, Decreto etc. – analogamente, para de forma adaptada, dar validade ao modelo, uma vez que não existe lei específica tratando o assunto.

Avaliando as possibilidades, utilizar a estratégia das jurisprudências não seria a opção mais interessante, pois jurisprudência é antes de tudo um entendimento legal, está sujeita a reinterpretação, podendo cada Tribunal julgar de acordo com seu entendimento e com isso gerar decisões diferentes. Mesmo a opção das súmulas não seria viável, visto que não existe súmula vinculante editada pelo Supremo Tribunal Federal, único órgão capaz de editar tal regulamento legal.

Para estabelecer procedimentos mais coesos com base legal estável para a questão da validação e autenticação dos *logs*, é preciso descartar a estratégia das jurisprudências. Então a solução proposta por este projeto é o uso da Infra-estrutura de Chaves Públicas do Brasil.

O ICP-Brasil ganhou força de Lei por meio da Medida Provisória 2200-2 em agosto de 2001. Essa Medida manteve sua validade por meio da Emenda Constitucional número 32, de 11 de setembro de 2001, que em seu art. 2º garante o vigor de todas as MP editadas em datas anteriores, até que Medida

Provisória ulterior as revogasse ou até deliberação definitiva do Congresso Nacional.

A partir de então, Resoluções, Decretos e Portarias foram editados para dar forma e validade legal ao ICP-Brasil. O ICP-Brasil é um conjunto de técnicas, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Isso significa dizer que o Brasil, através do ICP-Brasil, possui condições de emitir, revogar e validar certificados digitais [ICP,2006].

Estabelecendo um paralelo com a vida real, infra-estrutura de chaves públicas foi criada para funcionar como um "cartório digital". Processos de reconhecimento de firma, validação e autenticação de documentos, que na vida real somente poderiam ser feitas por um cartório autorizado, são supridos no mundo virtual por uma ICP, dando assim valor probante ao documento digital [MARCACINI,1999].

Uma infra-estrutura destas garante isso baseando-se em dois braços: técnicas e políticas de utilização. As técnicas englobam os algoritmos matemáticos e de criptografia, bem como o esquema de troca, criação e revogação de chaves criptográficas. Já as políticas concernem aos processos de segurança dos servidores e da infra-estrutura. As políticas existem para dar confiabilidade à solução como um todo.

As infra-estruturas de chaves públicas recebem esse nome por trabalhar com um par de chaves criptográficas, uma pública e outra privada. Falando um pouco de criptografia, existem dois esquemas criptográficos: os simétricos e os assimétricos. Nos simétricos, a mesma chave utilizada para cifrar a mensagem precisa ser utilizada para decifrar (a chave sempre precisa ser "privada").

Já os assimétricos utilizam o par de chaves: a pública, que pode ser distribuída livremente, e a privada, que precisa ser armazenada em local

seguro. Quando uma dessas chaves criptografa, somente a outra decodifica. Exemplo: João cifra a mensagem que escreveu para Ana com sua chave privada. Somente a chave pública de João poderá decifrar a mensagem; ou seja, Ana só conseguirá ler essa mensagem se ela estiver de posse da chave pública de João.

De toda a solução brasileira de chaves públicas, o esquema a ser utilizado, com a finalidade de validar a captura do tráfego e dar segurança ao processo de armazenamento, será a assinatura digital. De forma genérica, a assinatura digital é definida como um conjunto de procedimentos matemáticos com a utilização de técnicas de criptografia que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados de computador (um arquivo, um e-mail ou uma transação) [FUNASA,2006].

Utilizando a infra-estrutura do ICP-Brasil atende-se o quesito da legalidade da solução, fazendo com que o tráfego armazenado seja "assinado digitalmente".

A assinatura digital é a solução técnica para validar o documento. Ela serve para afirmar se o documento sofreu algum tipo de alteração depois do cálculo da assinatura. A assinatura é calculada utilizando duas funções matemáticas.

A primeira função é conhecida como função *hash*. Essa função é um algoritmo *one-way*, ou seja, é um algoritmo que efetuado o cálculo e gerado o *hash* não pode ser desfeito; não existe maneira de, a partir do *hash,* chegar ao conteúdo original que o gerou.

É uma função que utiliza como entrada dados de tamanhos variados, produzindo uma chave de tamanho fixo (*digest*, no nosso caso *traffic digest*) [HARRIS,2005]. Essa chave é um código binário que varia entre 8 e 1024 bits, dependendo do algoritmo utilizado.

Obrigatoriamente, todos os bits do documento devem contribuir para o cálculo do *hash*. Isso significa que a alteração de qualquer bit no documento vai mudar o *hash* produzido [PERKO,2004].

Tecnicamente a assinatura digital é calculada utilizando dois elementos. Primeiro, conforme explicado do parágrafo anterior, dá-se o cálculo do "*traffic digest*" através de uma função *hash*, utilizando como valores de entrada o fluxo de tráfego a ser armazenado. O segundo passo é criptografar o *digest* com a chave privada do assinante (criptografia assimétrica).

Para fazer a validação são necessários: o documento a ser verificado e sua assinatura digital. Na validação, primeiro é calculado o *digest* utilizando como entrada o documento em questão. Na segunda parte do processo, a assinatura digital é decifrada utilizando a chave pública do par de chaves. O produto desse cálculo é o *digest* anterior. É feita uma comparação dos dois *digests* e, se forem coincidentes, pode-se afirmar que o documento não foi alterado. A figura a seguir exemplifica melhor o processo.

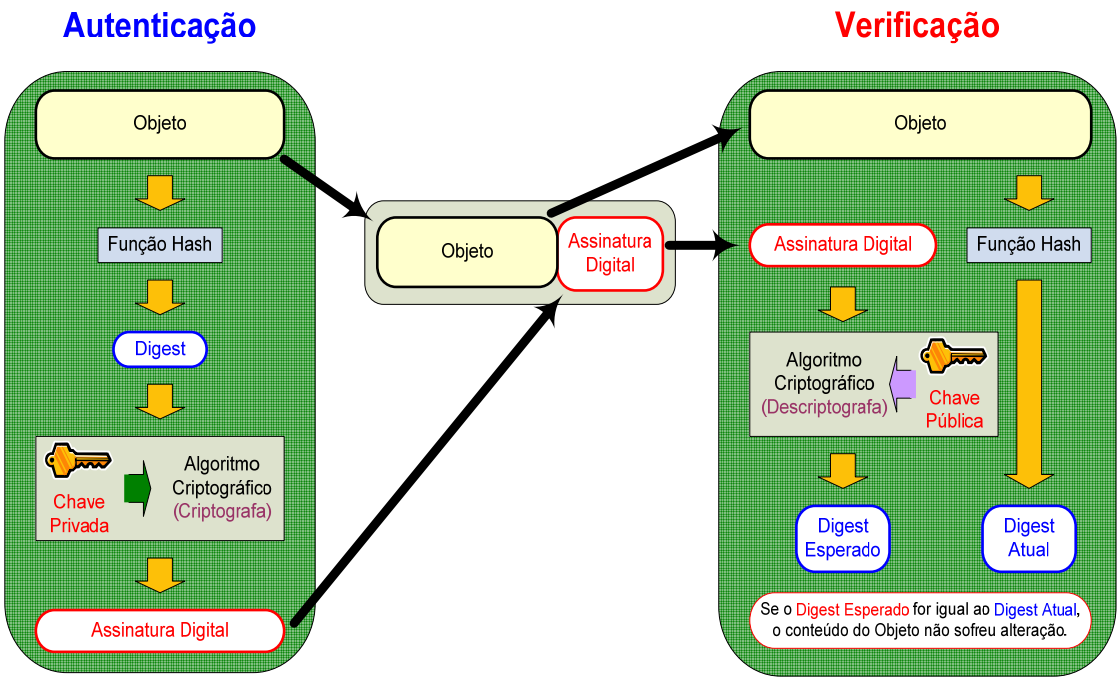


Figura 9 – Esquema de funcionamento para assinatura digital.

Assim, pode-se concluir que a questão da legalidade para a captura, armazenamento e autenticação do tráfego está preenchida. O próximo assunto a ser abordado é do mecanismo de captura e de armazenamento.

4.4 COMO ARMAZENAR

4.4.1 Captura

Os Sistemas de Prevenção de Intrusão, conforme visto, são soluções com posição privilegiada na rede – em linha –, fazendo com que todo o tráfego a ser analisado passe pelo equipamento. A análise desse tráfego é efetuada em tempo real. A idéia seria fazer uma cópia desse tráfego e armazená-lo em um banco de dados. Essa cópia deverá ser enviada ao banco de dados de armazenamento do tráfego. O banco de dados obrigatoriamente deverá ser disponibilizado em um equipamento físico diferente do que faz a análise. Essa característica dá maior segurança à solução como um todo, uma vez que, se o dispositivo de análise e bloqueio for comprometido em um ataque, o banco com a cópia do tráfego estará seguro.

O envio da cópia do tráfego deverá ser feito por uma interface de rede diferente das interfaces que fazem a análise, já que estas não possuem pilha TCP/IP. Por questão de economia de recursos físicos, o envio pode ser efetuado pela interface de gerenciamento, de preferência em um canal seguro. Entenda-se por canal seguro, um túnel criptografado ponto-a-ponto entre o dispositivo de análise e o dispositivo de armazenamento forense do tráfego.

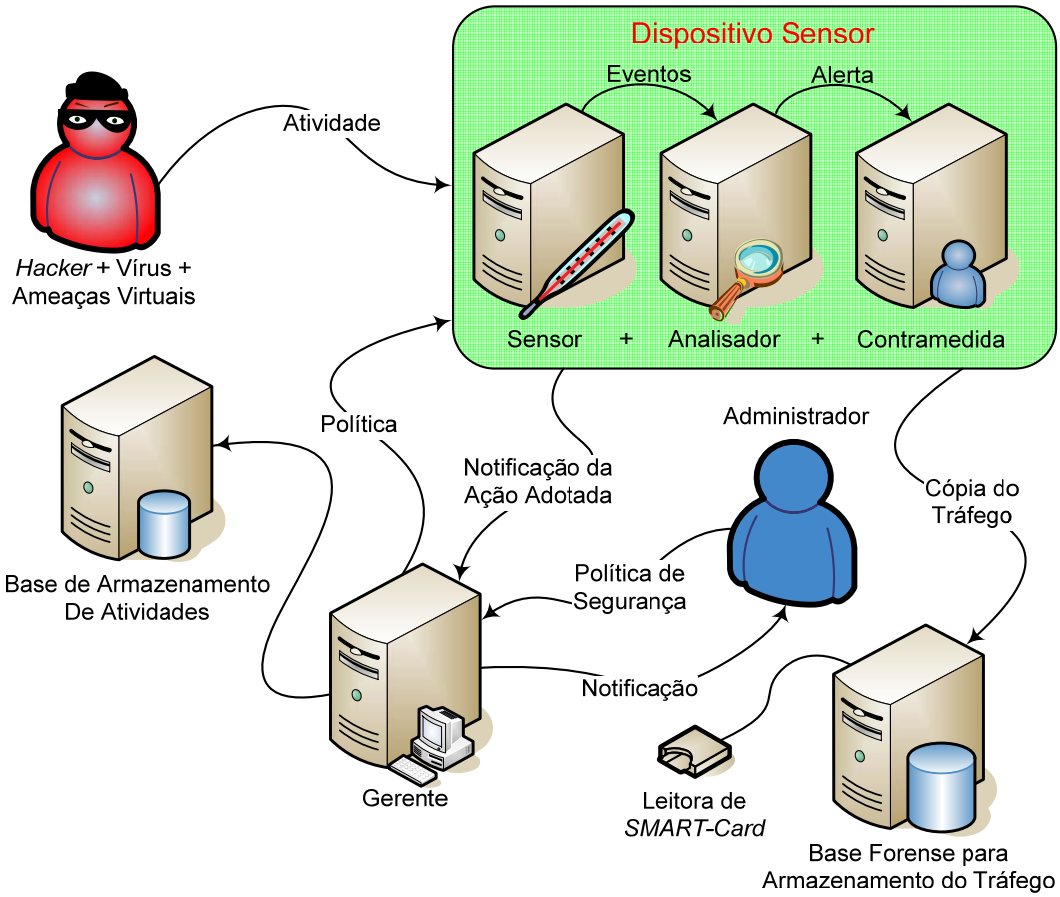


Figura 10 – Modelo de IPS com proposição para adição da base forense.

4.4.2 Armazenamento

Definido o quê armazenar, é necessário definir "como" armazenar. Como armazenar precisa atender a alguns requisitos. Inicialmente, precisa estar em sincronia com a legislação vigente, precisa também de um mecanismo para capturar o tráfego seguido de um outro mecanismo para armazenar o tráfego capturado de forma segura, depois garantir autenticidade ao conteúdo armazenado. Por último e não menos importante, precisa permitir a recuperação rápida desse tráfego armazenado.

Por suas técnicas de armazenamento e funcionamento, a proposta para este modelo computacional é a utilização de um banco de dados relacional. Bancos relacionais são tecnologias sedimentadas, utilizados em larga escala, que possuem como principais vantagens o controle de redundância de meta dados, o compartilhamento de dados multi-usuário com controle de

concorrência, a restrição a acesso não autorizado, a tolerância a falhas e, finalmente, a capacidade de representar relacionamentos complexos entre dados [UNIMAR,2000].

Os dois principais problemas no uso desse sistema estão no custo e na necessidade de profissionais qualificados para administração.

Os dados foram divididos em três grupos de tabelas. O primeiro é uma referência ao que os IPS já fazem. Essa tabela vai guardar informações sobre as ocorrências dos ataques, armazenando endereço e portas de origem e de destino, em que ataque aquele tráfego se enquadrou, data, hora, assinatura digital e informações relativas à ocorrência.

O segundo grupo seria referente aos possíveis ataques, que sistemas, aplicações e protocolos afetados. O último seria a tabela com a cópia do tráfego, armazenando o fluxo do tráfego. Ela é a razão dessa proposta de modelo computacional.

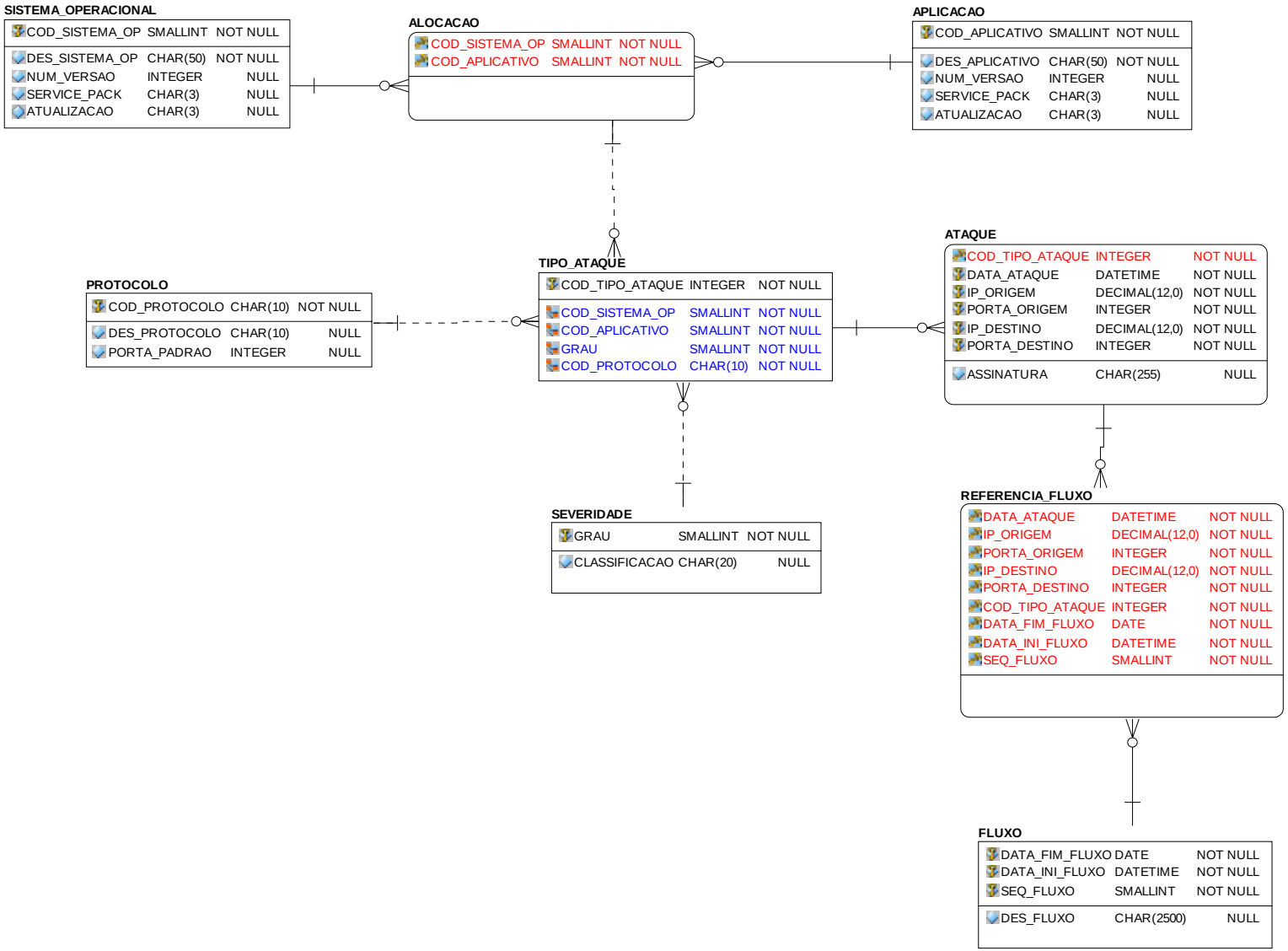


Figura 11 – Modelo Entidade Relacionamento do Banco Forense

4.5 ESQUEMAS DO MODELO

A figura 12 mostra o fluxo do pacote em um sensor IPS.

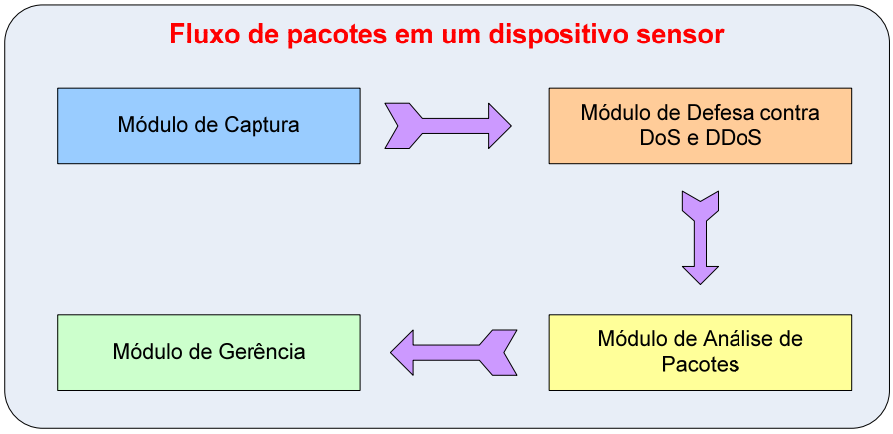


Figura 12 – Fluxo dos pacotes em um sensor IPS.

O tráfego entra pelo módulo de captura, segue para o primeiro algoritmo de defesa contra ataques de negação de serviço e negação de serviço distribuído. Passando por esse módulo o pacote segue para uma análise mais apurada, onde é feita a reorganização dos pacotes, montagem do fluxo, verificação de ataques por anomalia e por último a verificação dos ataques por assinatura. Tendo passado os módulos de análise, o pacote segue para o módulo de gerência, aonde ele, no caso de ser um pacote malicioso, será descartado e o *checksum* da conexão TCP recalculado; ou, no caso de não ser malicioso, seguirá seu caminho para o endereço de destino.

Tratando cada um dos casos propostos, a seguir o esquema físico-lógico da proposição fluxo completo.

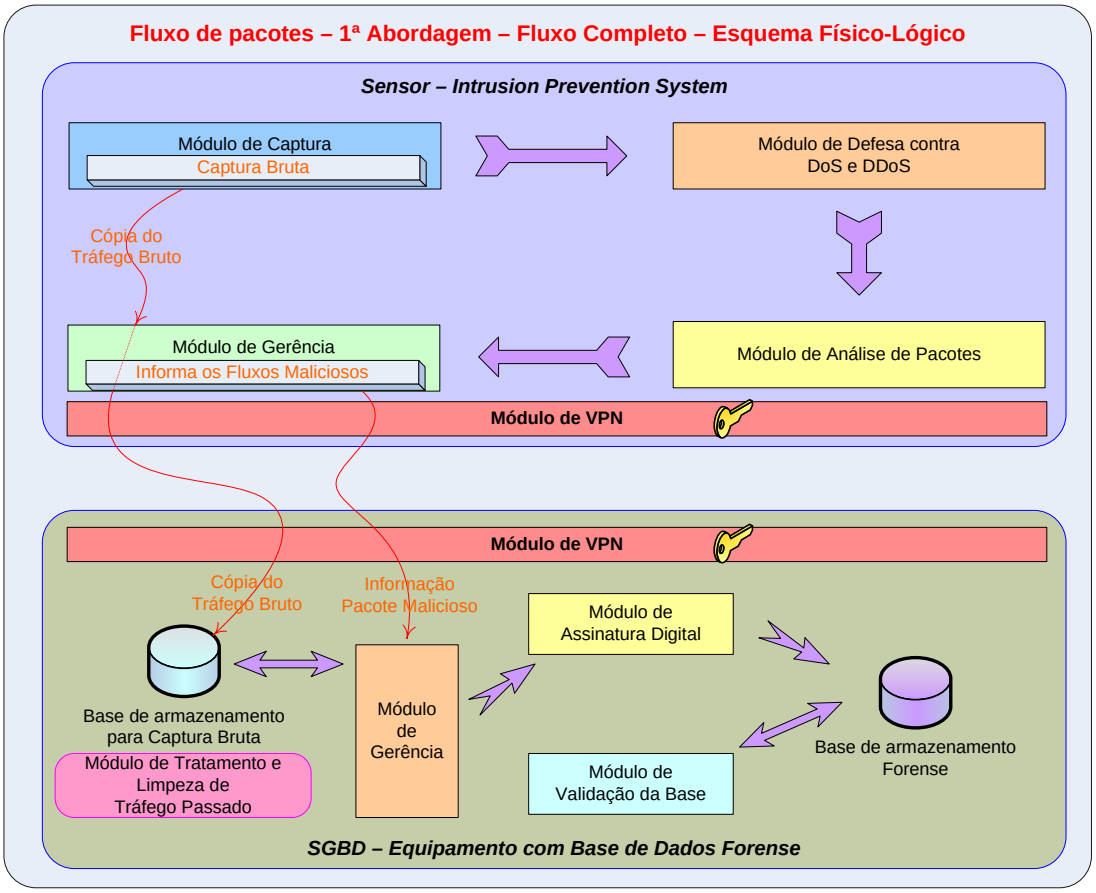


Figura 13 – Esquema Físico-lógico – Captura do fluxo completo.

Nessa abordagem seria necessária a alteração em dois dos quatro módulos do Sensor. A primeira seria no módulo de captura, para efetuar cópia dos pacotes, enviando-os diretamente para o módulo de gerência. A segunda alteração é no módulo de gerência para que ele repasse a cópia do fluxo vindo do módulo de captura, para a base de armazenamento de captura bruta. Outra alteração se faz necessária nesse módulo, para informar ao módulo de gerência da Base de dados forense qual fluxo contém pacote malicioso.

Segue detalhamento de cada elemento da figura 13.

Captura bruta, Sensor – Componente de software a ser adicionado no módulo de captura do Sensor, para fazer cópia e encaminhamento do tráfego para o módulo de gerência.

Informa fluxo malicioso, Sensor – Componente de software a ser adicionado

para encaminhar a cópia do tráfego ao equipamento forense e informá-lo de fluxos com pacotes maliciosos.

Módulo VPN, Sensor – Componente de software responsável pelo estabelecimento do túnel criptográfico entre o sensor e equipamento com a base forense.

Módulo VPN, Forense – Componente de software responsável pelo recebimento da requisição de estabelecimento do túnel com o sensor.

Módulo de tratamento e limpeza de tráfego passado, Forense – Algoritmo responsável pela exclusão dos fluxos de tráfego da base de captura bruta.

Módulo de gerência, Forense – Algoritmo responsável pelo recebimento da informação de tráfego malicioso do sensor, bem como a consulta desse fluxo na base de captura bruta e seu encaminhamento para o módulo seguinte, a assinatura digital.

Módulo de assinatura digital, Forense – Na inicialização este módulo deve efetuar a leitura da chave privada no *smart-card*. Essa chave será armazenada em memória volátil, devendo o *smart-card* ser retirado da leitora e armazenado em local seguro. Esse módulo fará a leitura do objeto de entrada: o tráfego, e efetuará o calculo da assinatura para o armazenamento definitivo na base forense.

Base Forense, Forense – Armazenará a ocorrência dos ataques, seus respectivos fluxos bem como a assinatura digital.

Módulo de Validação da Base Forense, Forense – Algoritmo de interface, responsável pela verificação, manutenção, consultas e não-comprometimento da base definitiva.

A figura 14 representa o esquema físico-lógico da segunda proposição.

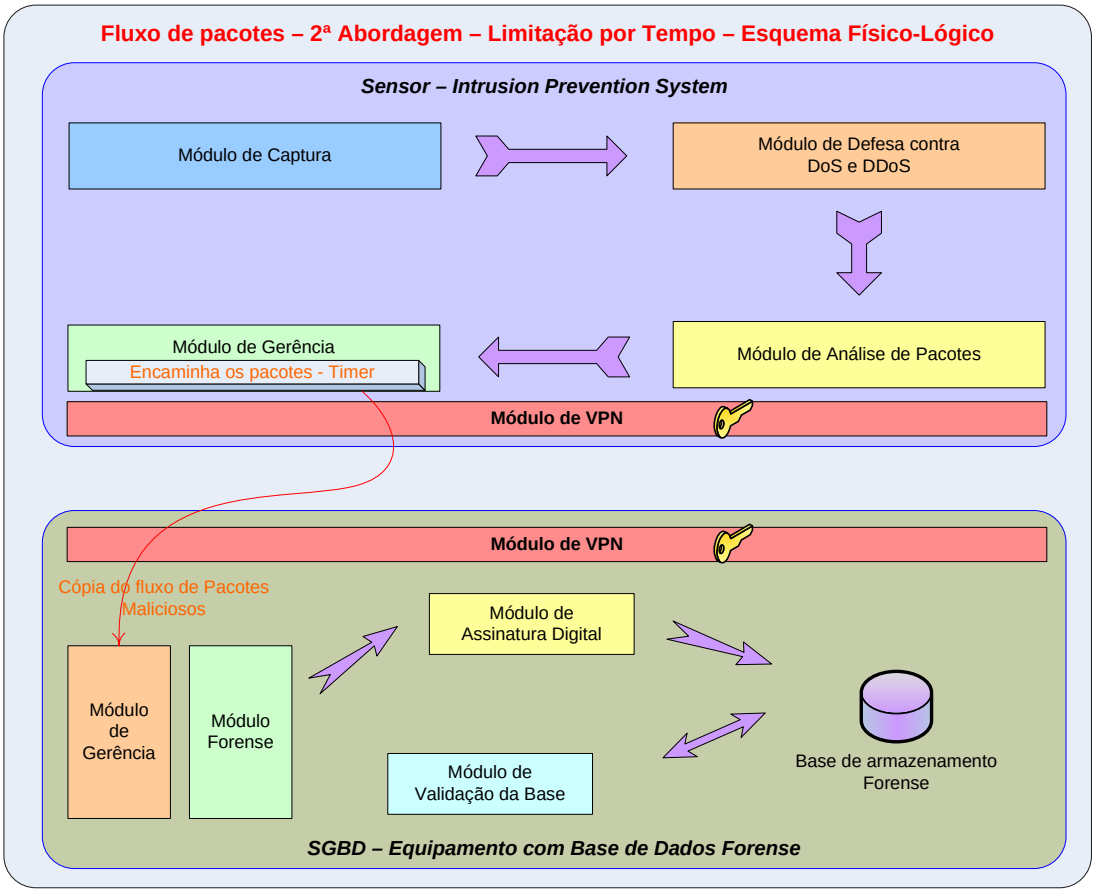


Figura 14 – Esquema Físico-lógico – Limitação da captura por tempo.

A diferença dos módulos entre a abordagem anterior e esta, é a exclusão da base de captura bruta e de seu módulo de limpeza, que nesta abordagem se tornaram desnecessários.

Encaminha os Pacotes, Sensor– Componente de software a ser adicionado no módulo de gerencia do sensor, com um timer para que caso um pacote malicioso seja detectado, o mesmo e os pacotes subseqüentes sejam encaminhados durante um tempo predeterminado para a base forense.

Módulo Forense, Forense – Esse algoritmo é responsável por analisar e agrupar os ataques oriundos de um endereço comum, dentro de uma mesma captura.

Os outros módulos continuam com a mesma função do módulo anterior.

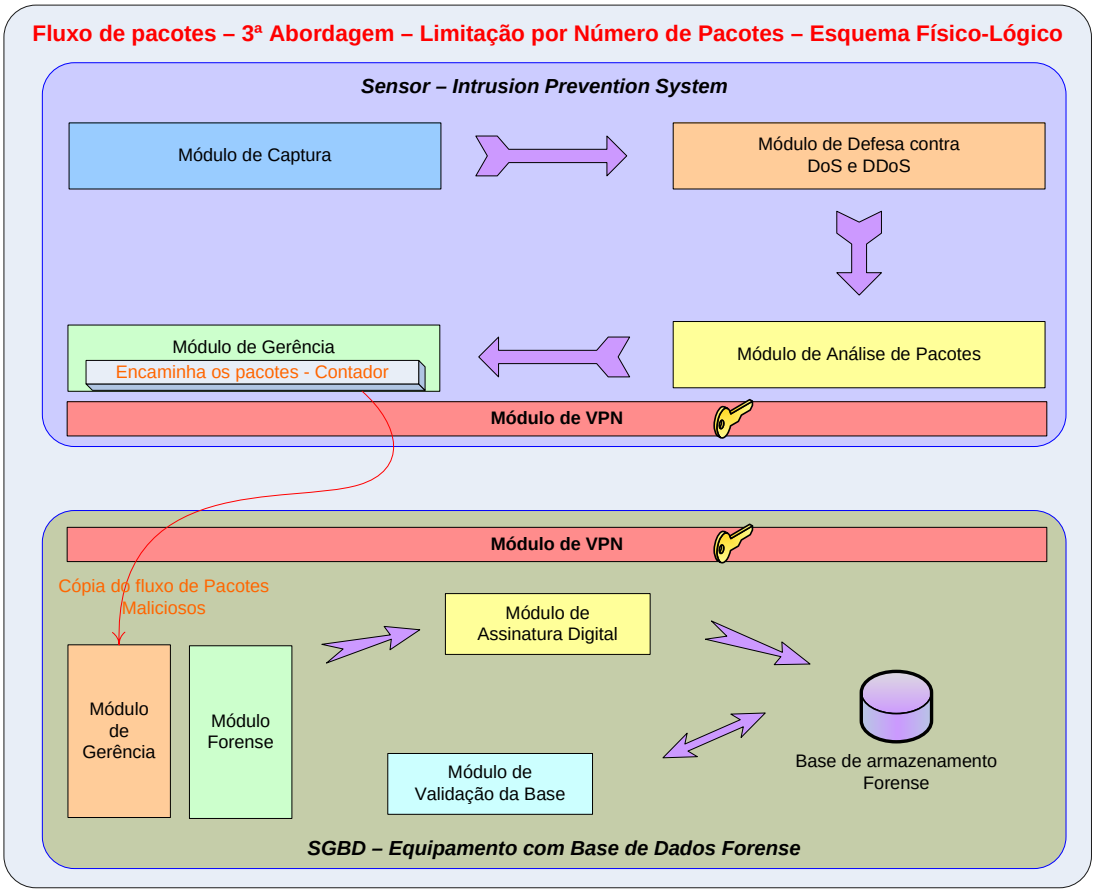


Figura 15 – Esquema Físico-lógico – Limitação da captura por número de pacotes.

A única diferença entre esta abordagem e a anterior, está no módulo de encaminhamento de pacotes que, em vez de limitar a captura por um timer, vai limitar a captura utilizando um contador com um número máximo de pacotes subseqüentes.

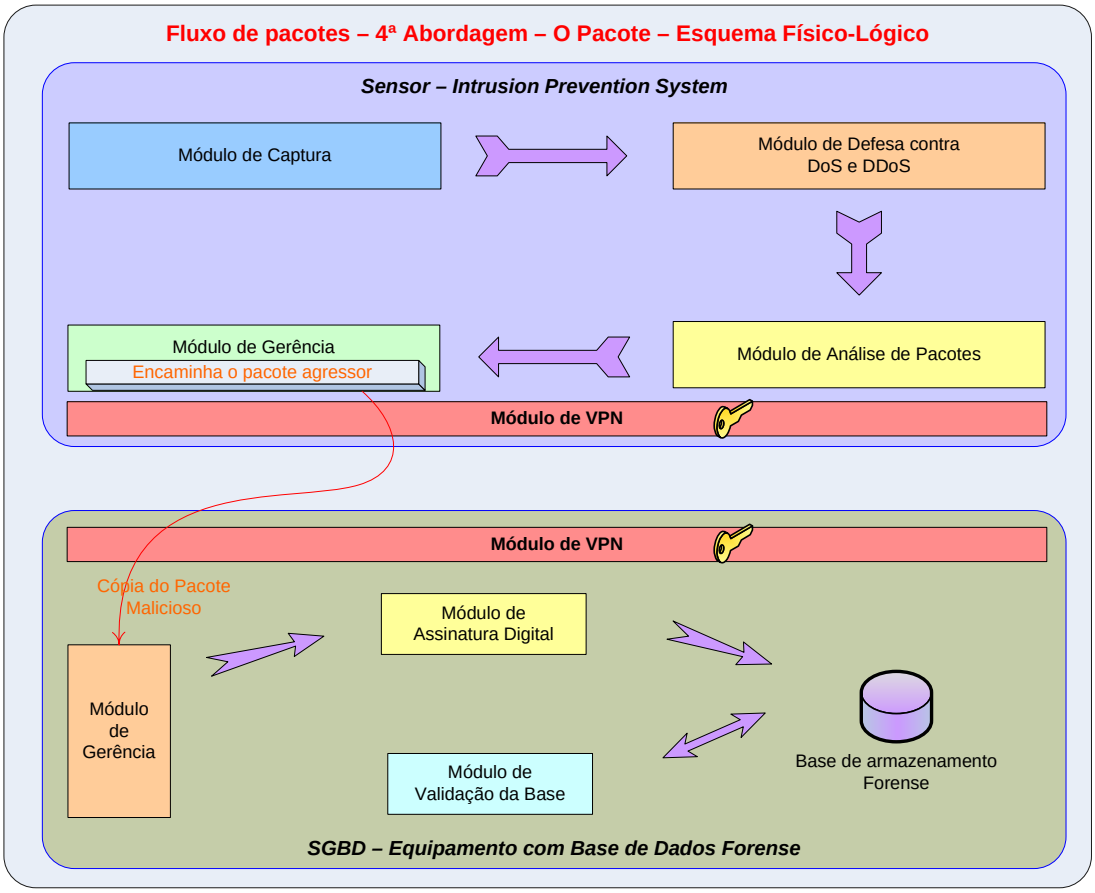


Figura 16 – Esquema Físico-lógico – Captura exclusiva do pacote agressor.

Nesta última abordagem é necessário apenas que o módulo de gerência do sensor encaminhe para o módulo de gerência da base forense cópia do pacote agressor.

4.6 DIAGRAMA DE ATIVIDADES

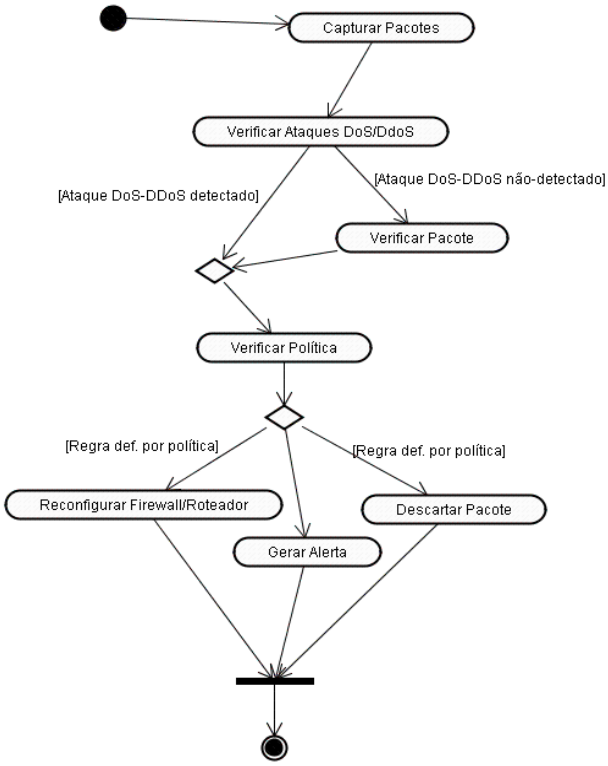


Diagrama 1 – Diagrama de atividades de um sensor IPS.

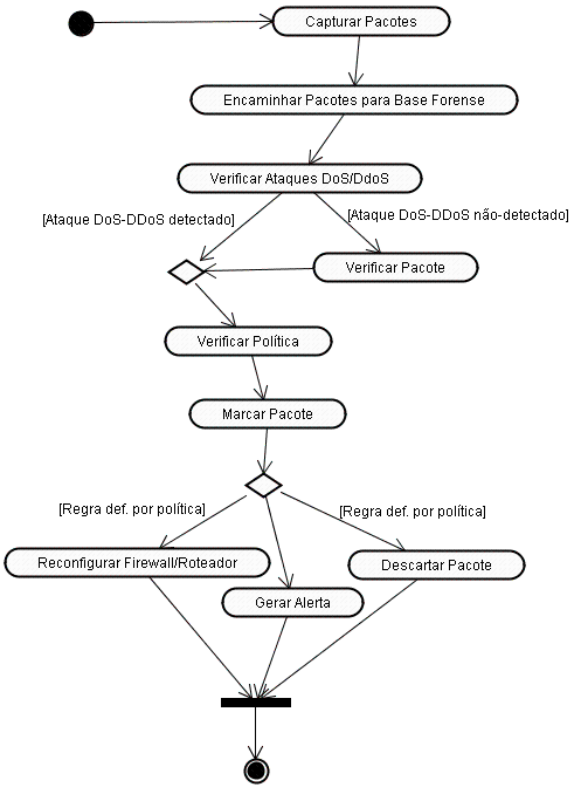


Diagrama 2 – Diagrama de atividades de um sensor IPS trabalhando na 1ª abordagem – Fluxo Completo.

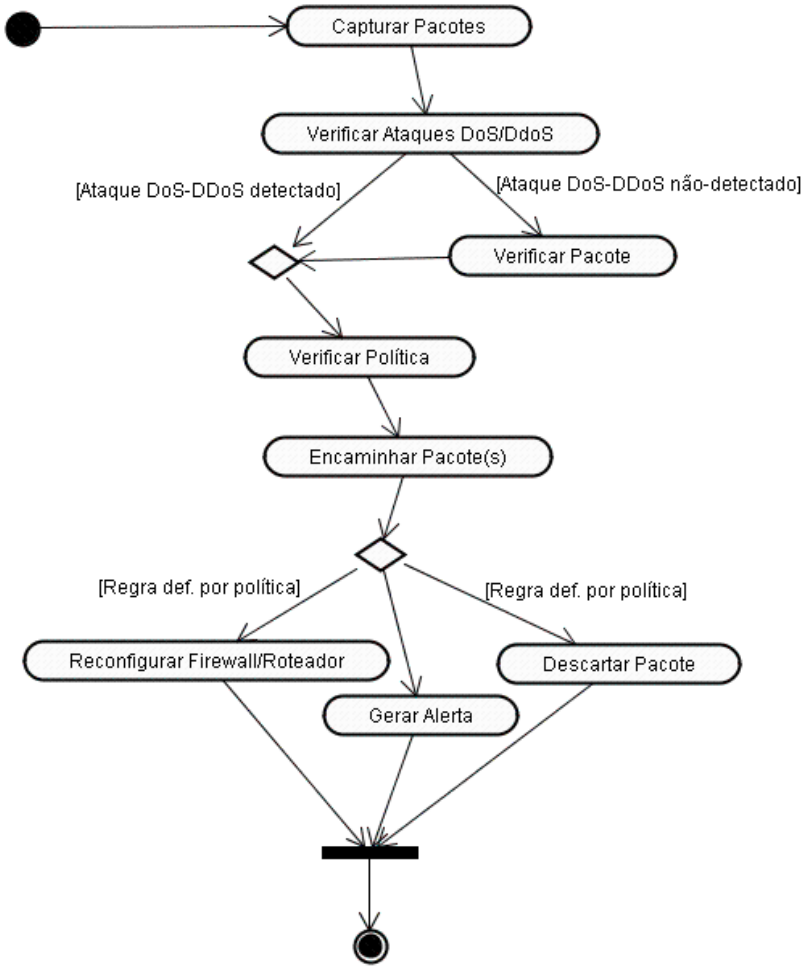


Diagrama 3 – Diagrama de atividades de um sensor IPS trabalhando na 2ª, 3ª e 4ª abordagens – Limitação por tempo, pacotes e cópia do pacote agressor.

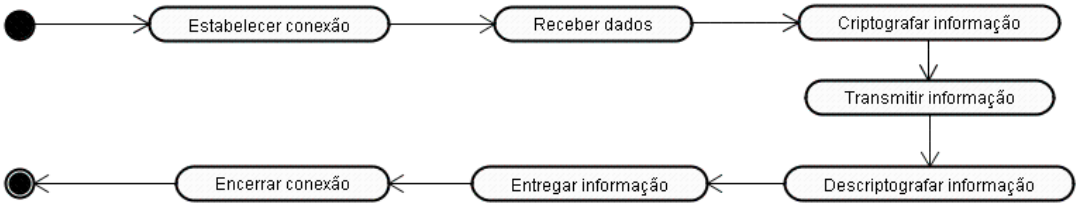


Diagrama 4 – Diagrama de atividades – Módulo VPN.

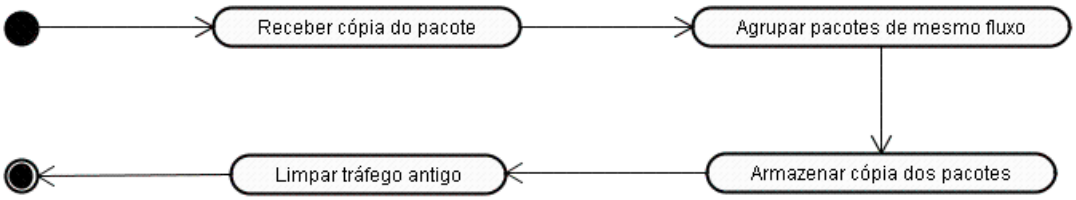


Diagrama 5 – Diagrama de atividades – Base de captura bruta – 1ª abordagem – Fluxo Completo.

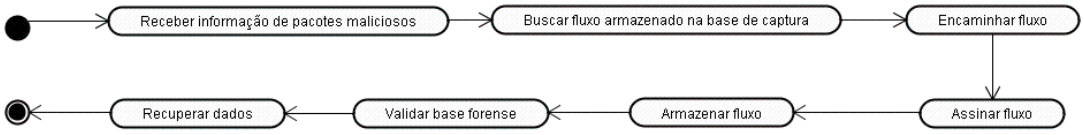


Diagrama 6 – Diagrama de atividades – Base forense – 1ª Abordagem – Fluxo Completo.

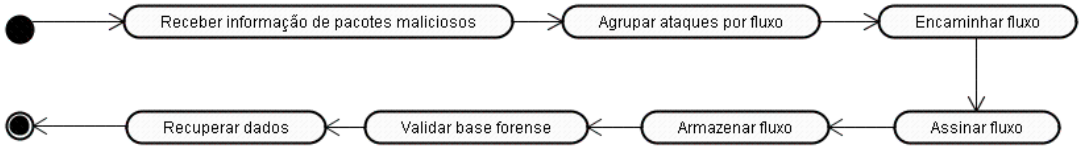


Diagrama 7 – Diagrama de atividades – Base forense – 2ª e 3ª abordagens – Limitação da captura por tempo e por número de pacotes.

4.7 VALIDAÇÃO DO MODELO

Na proposição deste projeto uma das bases de sustentação foi definida pela percepção da evolução dos sistemas de detecção para os de prevenção. O atendimento às demandas de um perito de forense computacional na execução de suas atividades foi o segundo braço. E, na união destes dois domínios de conhecimento, o projeto tomou forma, por meio de um modelo técnico com sólida base legal. Uma importante etapa para consolidar um projeto é estabelecer uma metodologia para validar os requisitos do modelo proposto. No caso em tela, a forma mais interessante de validação seria a implementação desse modelo em protótipo. Entretanto, essa metodologia, apesar de mais indicada, mostra-se inviável em virtude do prazo de desenvolvimento ser incompatível com um projeto dessa amplitude, sobretudo pelo grande número de tecnologias envolvidas no processo de implementação, bem como pelo nível de detalhamento de cada uma delas.

A metodologia escolhida e adotada foi a elaboração e aplicação de questionário à analistas de sistemas que trabalham com segurança da informação e peritos de forense computacional. O questionário era composto por questões relativas ao problema da validação dos *logs,* ao tempo elevado para busca de informações em bases de dados com tráfego de rede e à proposição do modelo em tela como resolução para estes problemas.

O questionário (Apêndice I) foi elaborado em formato pdf com intuito de priorizar o seu preenchimento de forma eletrônica. A pesquisa foi realizada entre os dias 21 de maio e 06 de junho. Os formulários foram remetidos para quinze entrevistados, onde doze responderam por correio eletrônico.

As perguntas de números um e dois dizem respeito às possíveis fontes de informação utilizadas pelo entrevistado quando do início dos procedimentos para análise forense. Já as perguntas três, quatro e cinco abordam a questão das ferramentas de busca e identificação de tráfego malicioso em base de informações e como ele avalia a velocidade desta busca. As perguntas seis e sete sintetizam os problemas que os peritos experimentam quando buscam informações de ataques, tendo em vista que o universo de busca é, normalmente, muito grande. Por fim, as perguntas oito e nove questionam o entrevistado acerca da solução dos problemas mencionados nas perguntas anteriores. A pergunta número dez resume a proposta do modelo.

Seguem os gráficos com análise:

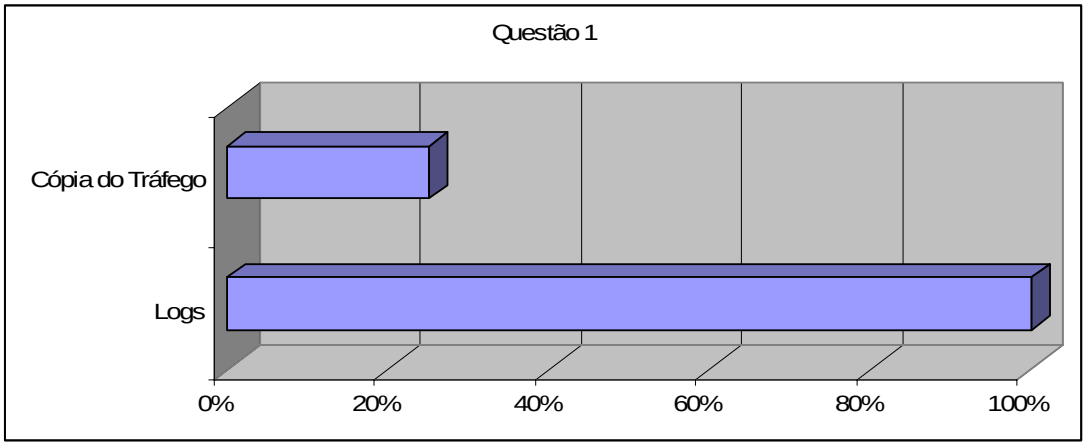


Gráfico 1 – Questão 1

A questão número um perguntava o que o entrevistado, na execução de suas atividades, utiliza como fonte de informações para a análise forense de rede. E como resposta o entrevistado poderia escolher *Logs*, Cópia do Tráfego e outros, especificando a opção. Dos entrevistados 25% responderam a opção cópia do tráfego, e 100% dos entrevistados afirmaram

utilizar *logs*. Nenhum deles sinalizou com alguma outra técnica ou recurso como fonte de informações.

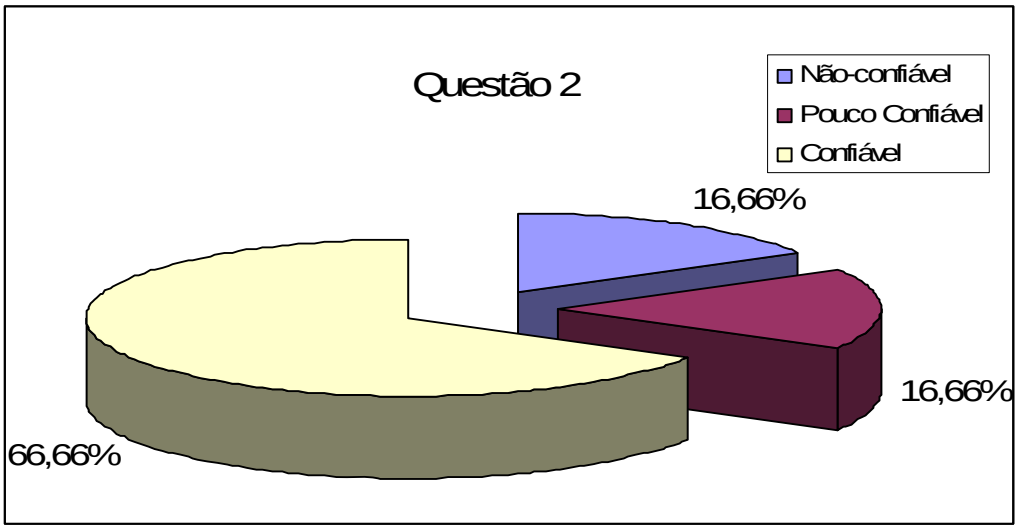


Gráfico 2 – Questão 2

Na questão 2, cujo objetivo era o de avaliar o grau de credibilidade da fonte de informação utilizada, a maior parte dos entrevistados considerou os *logs* e a cópia do tráfego como fontes confiáveis de informações para execução de suas tarefas.

As questões três e quatro eram questões com respostas livres e subjetivas. Tinham dois objetivos: primeiro, determinar se os entrevistados utilizavam ferramentas para pesquisa em suas fontes de informação e, segundo, determinar se os entrevistados utilizavam alguma técnica ou ferramenta específica para filtragem de informação na busca em bases textuais (*logs*). O índice de respostas a essas questões foi baixo. O resultado dessas questões não representou nenhuma lacuna no objetivo final do questionário, pelo contrário, atendeu às expectativas, visto que essa ausência de respostas corrobora à base argumentativa desse projeto, no que se refere as dificuldades enfrentadas para pesquisa de ataque em bases textuais. A pergunta número três era: Qual ferramenta você utiliza para busca e identificação de informações sobre ataques e atacantes recorrentes nos *logs*, base de dados ou em outras fontes de dados? E a pergunta número quatro era: Qual técnica/ferramenta você utiliza para diferenciar acesso

normal e eventos malignos dentro do universo de tráfego capturado por um dispositivo de análise forense de rede?

A questão cinco abordava o entrevistado acerca da velocidade em que se dá a busca e identificação de eventos nestas bases de dados. A grande maioria acredita que o tempo para a busca e identificação é muito elevado.

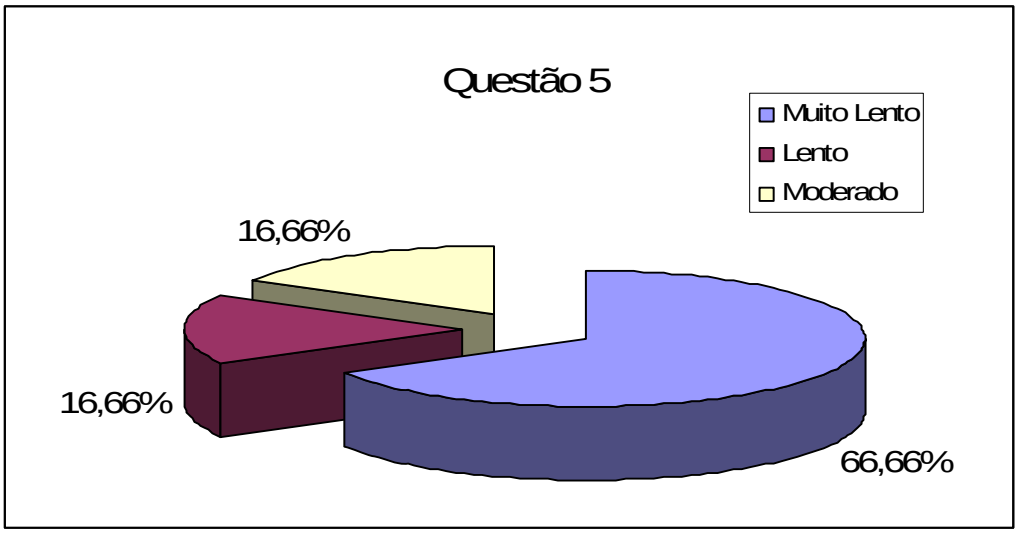


Gráfico 3 – Questão 5

A questão número seis perguntava, considerando o universo de *logs* analisados, qual o percentual de ataques – efetivamente identificados – e se estes poderiam servir como auxiliar na solução de um crime. A grande maioria acredita que menos de 5% dos *logs* são realmente aproveitáveis para auxiliar na resolução de um crime.

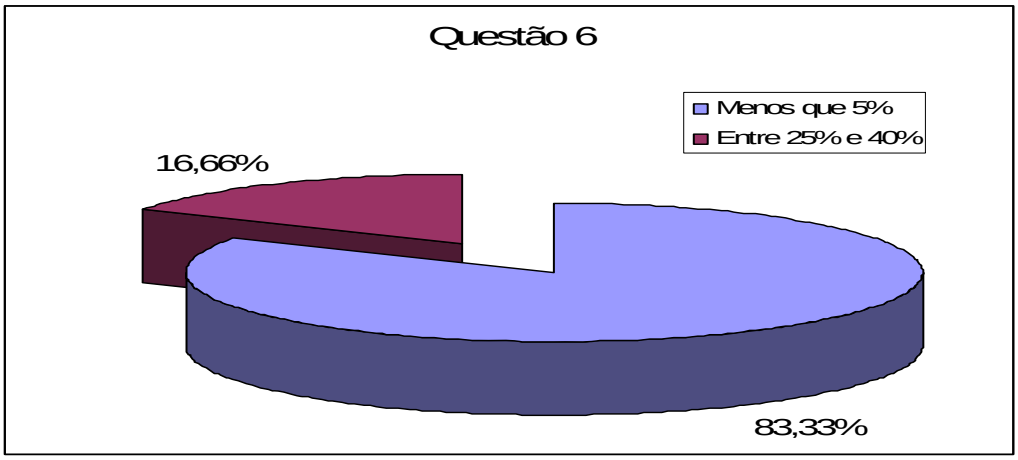


Gráfico 4 – Questão 6

A questão sete tratava da avaliação do grau de consistência das informações disponibilizadas apenas por *logs*. Metade dos entrevistados respondeu que informações disponibilizadas somente por *logs* tinham pouca consistência para uma avaliação mais profunda do ataque. Já a outra metade acredita que as informações disponibilizadas por *logs* são suficientemente consistentes para uma análise forense.

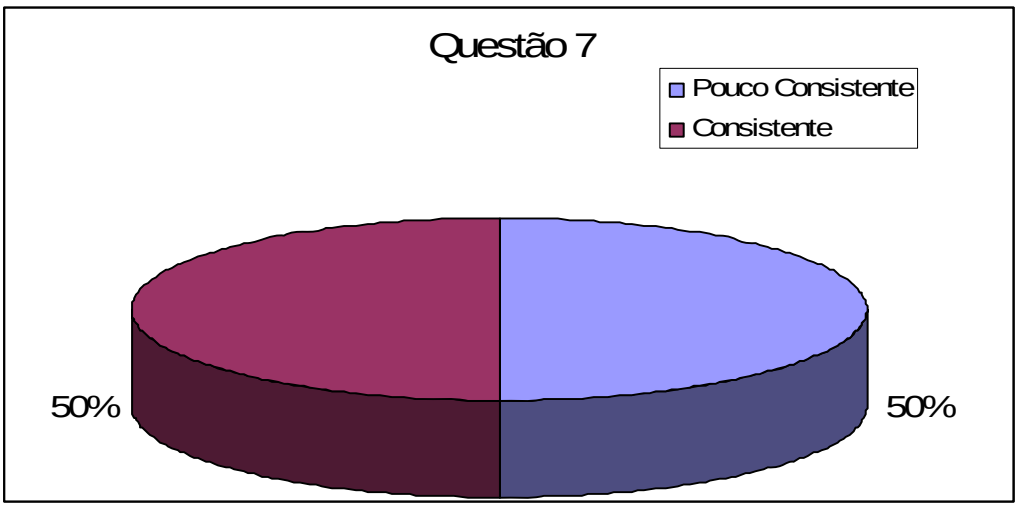


Gráfico 5 – Questão 7

A questão oito perguntava acerca da utilidade de uma ferramenta capaz de fazer a separação entre tráfego normal e tráfego malicioso. A maioria absoluta dos entrevistados acredita ser muito útil, 16,66% avaliou como extremamente útil.

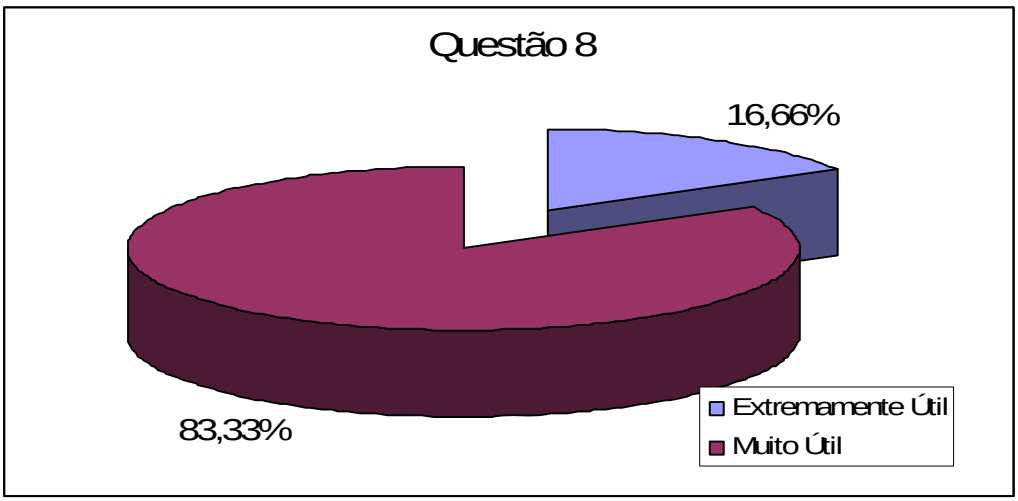


Gráfico 6 – Questão 8

A questão nove amplia o cenário proposto na questão anterior com a possibilidade de uma ferramenta que, além de efetuar o *log* do evento malicioso, efetuasse a cópia do tráfego, garantindo assim mais informações ao analista. A maioria acredita ser extremamente útil.

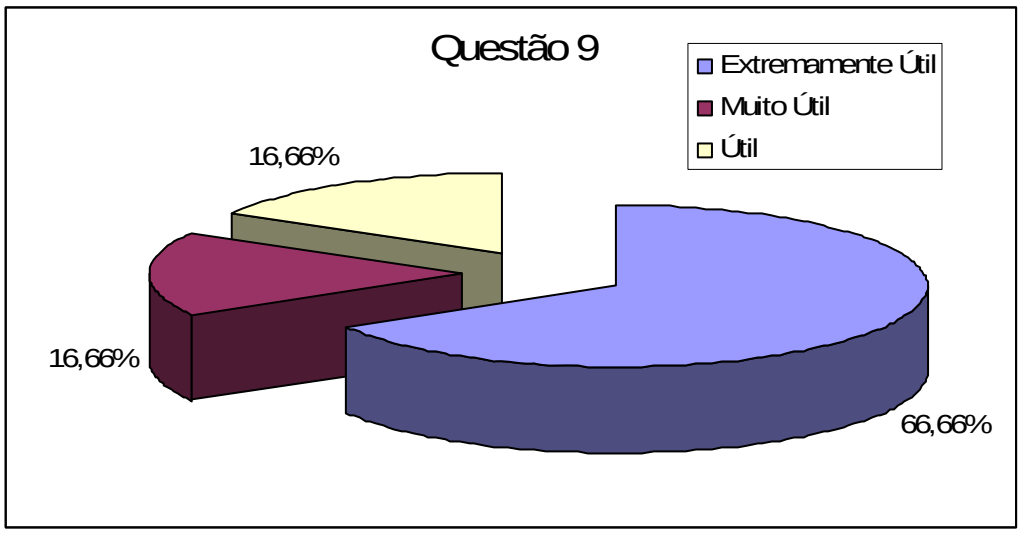


Gráfico 7 – Questão 9

A última questão trata do grau de credibilidade que o entrevistado atribuiria a uma ferramenta que, além de efetuar o registro do ataque, armazenasse cópia do tráfego, assinando digitalmente essa cópia. Dos entrevistados 83,33% escolheram a opção “muito confiável” e 16,66% consideraram como “totalmente confiáveis”.

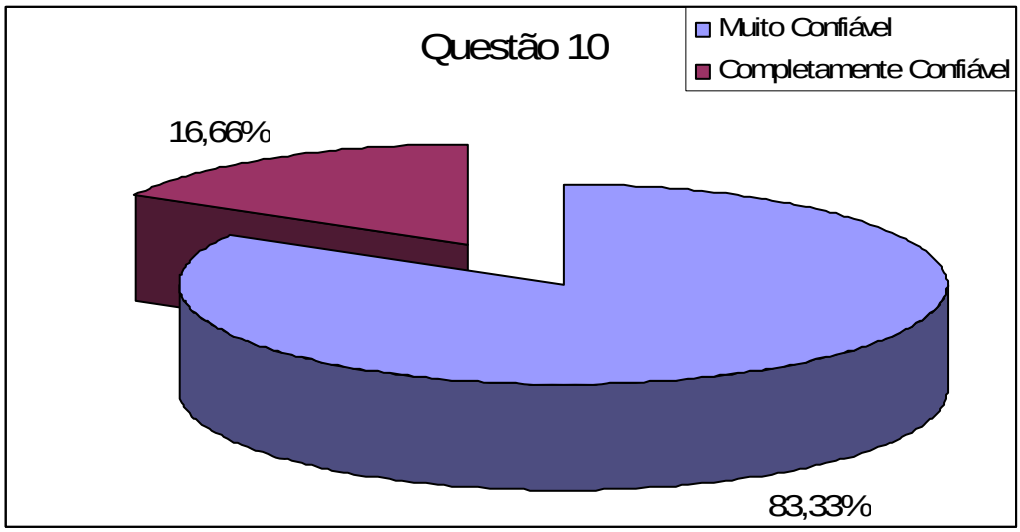


Gráfico 8 – Questão 10

Efetuando-se um estudo mais detalhado do questionário, suas perguntas e respostas, pode-se perceber que o assunto em tela envolveria com facilidade um número maior de questões específicas e maior detalhamento técnico. Entretanto devido a limitação do *corpus* do projeto em questão, o questionário atendeu a necessidade de avaliar os requisitos do modelo e sua funcionalidade.

4.8 TRABALHOS FUTUROS

Como proposta para trabalhos posteriores a sugestão seria para a definição do funcionamento interno de cada um dos módulos propostos por este modelo, bem como das interfaces para troca de mensagens entre os referidos módulos, seguindo as recomendações definidas pelo IDWG.

CONCLUSÃO

Novas linhas de pesquisas e o constante desenvolvimento em segurança da informação têm, de uma maneira geral, contribuído para o amadurecimento das soluções de prevenção de intrusão. O Gartner Group, maior grupo de consultoria independente para pesquisa em tecnologia da informação, publica de dois em dois anos estudo, conhecido no mercado como quadrante mágico. O qual avalia e indica, num *ranking*, a posição dos principais fabricantes sobre determinada tecnologia. O quadrante mágico publicado no segundo semestre de 2003 (Anexo I), analisou os principais fabricantes de sistemas de detecção de intrusão. No quadrante mágico publicado no biênio seguinte (Anexo II), o Gartner Group deixou de analisar as soluções puramente de detecção de intrusão, focando seu estudo nos *appliances* de prevenção de intrusão. Nesta última publicação, o Snort, produto de código aberto e muito utilizado nas corporações, foi retirado do estudo por ter sido considerado ultrapassado.

A padronização das interfaces, protocolos de comunicação e funcionamento das diversas soluções dos sistemas contra intrusão é ponto positivo. Facilitará a troca de mensagens e o ganho da segurança para o ambiente coorporativo como um todo, uma vez que os fabricantes poderão focar energia e investimento em melhorias da solução, tais como algoritmos de *data mining* (mineração de dados), inteligência artificial e redes neurais, os quais poderão ser utilizados para prover maior qualidade às soluções de prevenção de intrusão.

Observando os trabalhos internacionais, pode-se perceber que a padronização não está muito longe. Os Internet-Drafts do IDWG completaram todos os requisitos para se tornarem RFC. E, apesar destes trabalhos não sinalizarem com tecnologias convergentes, na competição pelo mercado consumidor os fabricantes utilizam estas propostas, muitas vezes acadêmicas, como tecnologias complementares a suas soluções.

O crescente e constante investimento nesta tecnologia sugere que em mais

ou menos tempo os desenvolvedores implementarão, se não alguma, todas as sugestões propostas no modelo deste projeto.

A evolução tecnológica é uma constante. Durante a execução deste projeto, a comunidade de código livre publicou a versão estável de um módulo para o Snort funcionar em linha. É um passo importante na sedimentação da tecnologia de prevenção de intrusão.

Traçando um paralelo da proposição deste modelo com o processo de medicina legal, seria como afirmar que, com o modelo proposto, o perito, além de possuir material para um exame forense inicial – os *logs* –, disporia também de um "corpo" – o tráfego – como prova cabal, de modo a dirimir quaisquer dúvidas, inclusive durante o processo judicial.

Com a cópia do tráfego e esse tráfego assinado digitalmente, este modelo provê ao perito a informação mais completa para que ele efetue estudo de caso. As possibilidades demonstradas no modelo em tela, uma vez efetivas, representariam avanço significativo na prevenção e identificação de crimes digitais, sendo possível um grande passo em direção ao estabelecimento e funcionamento da legislação especifica contra crimes eletrônicos.

Concluindo, pode se perceber que embora tenham sido atendidos, em todas as suas etapas, os requisitos da proposição inicial deste projeto acadêmico, existem melhorias a serem realizadas. Uma dessas melhorias corresponde à ampliação do cenário de avaliação técnica, implementação e funcionalidade.

REFERÊNCIAS BIBLIOGRÁFICAS

[AND,1972] – ANDERSON, James P. **Computer Security Technology Planning Study**. Volume 2 – Divisão de Sistemas Eletrônicos – Out. 1972, Disponível em: http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf – Visitado em jan./2006

[AND,1980] – ANDERSON, James P. **Computer Security Threat Monitoring and Surveillance**. Trabalho publicado para Força Aérea Americana em Abr. 1980 – Disponível em: http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf – Visitado em jan/2006.

[ANDREA,2004] – D´ANDREA, Edgar. **Ameaças e Vulnerabilidades**. Artigo publicado na revista ITWeb. Jul. 2004, Disponível em: http://www.itweb.com.br/solutions/gestao_empresarial/seguranca/artigo.asp?id=51208 – Visitado em jan/2006.

[ARIST,1973] – ARISTÓTELES. **Ética a Nicômaco**. Coleção Os Pensadores – Livro IV – Abril Cultural – 1ª Edição – Rio de Janeiro, Brasil – Jan. 1973

[BLUM,2004] – BLUM, Renato M. S. Opice e ABRUSIO, Juliana Canha. **Crimes Eletrônicos**. Artigo publicado na Revista Evidência Digital, ANO I nº. 1 – Jan. 2004, página 6, Disponível em: http://www.guiatecnico.com.br/evidenciadigital. – Acessado em dez/2005.

[CAMPELLO,2001] – CAMPELLO, Rafael Saldanha e WEBER, Raul Fernando. **Sistemas de Detecção de Intrusão**. Capítulo 1 – Instituto de Informática – Universidade Federal do Rio Grande do Sul – UFRGS – 2001, página 10

[CASEY,2004] – CASEY, Eoghan. **Digital Evidence and Computer Crime**. Academic Press, San Diego, 2ª. Ed. California, 2004.

[CHACON,2004] – CHACON, Adilson e outros. **IDS e IPS**. Seminário de Segurança de Redes – Universidade Católica de Pernambuco, 2º Semestre – 2004 – Disponível em: http://www.dei.unicap.br/~almir/se.2/ts04/ipsids/index.html – Visitado em dez/2005.

[CIDFA,1999] – PORRAS, Phil; SCHNACKENBERG, Dan; STANIFORD-CHEN, Stuart; DAVIS; STILLMAN, Maureen; WU, Felix. **The Common Intrusion Detection Framework Architecture**. – Disponível em: http://www.isi.edu/gost/cidf/drafts/architecture.txt – Visitado em jan/2006

[CISL,1999] – PORRAS, Phil; SCHNACKENBERG, Dan; STANIFORD-CHEN, Stuart; DAVIS; STILLMAN, Maureen; WU, Felix. **The Common Intrusion Specification Language**. – Disponível em: http://www.isi.edu/gost/cidf/drafts/language.txt – Visitado em fev/2006

[COULL,2003] – COULL, Scott; BRANCH, Joel; SZYMANSKI, Boleslaw; BREIMER, Eric. **Intrusion Detection: a Bioinformatics Approach**. Rensselaer Polytecnhnic Institute & Siena College – Agosto 2003 – Disponível em: http://www.cs.rpi.edu/~szymansk/papers/acsac03.pdf – Visitado em mar/2006.

[DENNING,1987] – DENNING, Dorothy E. **An intrusion-detection model**. IEEE Transactions on Software Engineering. Fev. 1987, páginas 222-232.

[FELIPPE,2002] FELIPPE, Donaldo J. **Dicionário Juridico** 15ª Ed. Campinas: Millenium 2002) p. 158

[FORWIKI,2006] – The Forensics Wiki. **"Network Forensics"** – Pesquisa no forensicswiki utilizando o termo "Network Forensicis" – Disponível em: http://www.forensicswiki.org/index.php/Network_forensics – Visitado em abr/2006

[FREITAS,2004] – FREITAS, Andrey Rodrigues de. **Terminologia Pericial**. Artigo publicado na Revista Evidência Digital, ANO I nº. 4 – Jan. 2004, página 6, Disponível em: http://www.guiatecnico.com.br/evidenciadigital. – Acessado em abr/2006.

[FUNASA,2006] – Funasa. **"Assinatura Digital"** – Pesquisa no site da Fundação Nacional da Saúde utilizando o termo "Assinatura Digital" – Disponível em: http://sis.funasa.gov.br/infcertificado/assinaturadigital.htm – Visitado em abr/2006

[HARRIS,2005] – HARRIS, Shon. **CISSP All-in-One Exam Guide, Third Edition (All-in-One)**. 3ª Edição – Ago/2005 – pp. 6 e 640.

[HEADY,1990] – HEADY, Richard; LUGER, George; MACCABE, Arthur e SERVILLA, Mark. **The architecture of a network level intrusion detection system**. Relatório técnico CS90-20, Departamento de Ciência da Computação – Universidade do Novo México, Ago/1990.

[HOWARD,1998] – HOWARD, John D.; LONGSTAFF, Thomas A. **A Common Language for Computer Security Incidents** (SAND98-8667). Livermore, CA: Sandia National Laboratories, 1998. Disponível em: http://www.cert.org/research/taxonomy_988667.pdf – Visitado em jan/2006.

[IBM,2006] – IBM. **"A mudança na natureza do crime"** – Pesquisa realizada em janeiro de 2006 com os executivos de alto escalão de mais de 3 mil empresas pelo mundo, sendo 450 só na América Latina. Publicada em abril 2006.

[ICP,2006] – ICP – Brasil. **"Infra-estrutura de Chaves Públicas – Brasil"** – Definição do ICP-Brasil – Disponível em: http://www.icpbrasil.gov.br/ – Visitado em abr/2006

[JONES,2006] – JONES, Keith J.; BEJTLICH, Richard; ROSE, Curtis W. **Real Digital Forensics – Computer Security and Incident Response** Addison-Wesley, Massachusetts 1ª Ed. EUA, 2006, pág. 75-83.

[KUMAR,1994] – KUMAR, Sandeep e SPAFFORD, Eugene H. **Classification A Pattern Matching Model for Misuse Intrusion Detection**. Anais da 17ª Conferência Nacional de Segurança da Computação, Out. 1994, páginas 11-21.

[KUMAR,1995] – KUMAR, Sandeep. **Classification And Detection Of Computer Intrusions**. Tese apresentada para obtenção do Título de Doutor em Filosofia – Universidade de Purdue, Ago. 1995, Disponível em: http://ftp.cerias.purdue.edu/pub/papers/sandeep-kumar/kumar-intdet-phddiss.pdf – Visitado em dez/2005.

[LI,2005] – LI, Wei. **Using Genetic Algorithm for Network Intrusion Detection**. – Departamento de Engenharia e Ciência da Computação – Maio 2005 – Mississippi State University – Mississipi – Estados Unidos – Disponível em: http://www.security.cse.msstate.edu/docs/Publications/wli/DOECSG2004.pdf – Visitado em mar/2006.

[LIRA,2005] – LIRA, Kaliane Wilma Cavalcante e CAVALCANTI, José Ivalmir Neves. **Crimes Praticados via Internet e suas Conseqüências Jurídicas**. Escola de Administração do Exército, Salvador-BA EsAEx – Artigo publicado na Revista Módulo Security Magazine, nº 414 – 14-Dez-2005 – Disponível em: http://www.modulo.com.br/pdf/crimes_virtuais.pdf – Acessado em dez/2005. Visitado em abr/2006

[MAIA,2004] – MAIA, Roberto Bomeny; SOARES, A. Alexandre de C.; LEÃO, Jorge Lopes de Souza. **Utilização da Lógica Difusa na Detecção da Intrusão**. Grupo de Teleinformática e Automação – Universidade Federal do Rio de Janeiro – Trabalho apresentado no WorkComp-2004 – Congresso de Ciências da Computação e Sistemas da Informação da Região Sul – Disponível em: http://www.gta.ufrj.br/~rmaia/SDDI.pdf – Visitado em mar/2006.

[MARCACINI,1999] – MARCACINI, Augusto Tavares Rosa. **"O Documento Eletrônico como Meio de Prova"** – Artigo publicado para o portal InfoJur. em 02/03/1999 – Disponível em: http://doneda.net/dinfo/doc/docelet_Marcacini.doc – Visitado em mai/2006.

[MARINONI,2004] – MARINONI, Luis Guilherme e ARENHONT, Sérgio Luis. **Manual do Processo de Conhecimento**, 3ª Ed. São Paulo: Revista dos Tribunais 2004, p. 311

[OLIVEIRA,1999] – OLIVEIRA, Frank Ned. **Sistemas de Detecção de Intrusão e Aspectos Legais**. Artigo publicado no Boletim Bimestral da RNP – NewsGeneration, Volume 3 nº 5. Set. 1999, Disponível em: http://www.rnp.br/newsgen/9909/ids.html – Visitado em dez/2005.

[OLIVEIRA,2002] – OLIVEIRA, Flávio de Souza; GUIMARÃES, Célio Cardoso; GEUS, Paulo Lício. **Um Framework para Preparação de Redes Windows 2000 para Futuras Análises Forense**. Capítulo 3 – Forense Computacional – Anais do IV Simpósio sobre Segurança em Informática 2002 – São José dos Campos, São Paulo, Brasil – página 102.

[PERKO,2004] – PERKO, Mitja. **" What exactly is hash and hash file?"** – Página no site de ajuda do aplicativo CDCheck 3.1.11.0 – Disponível em: http://www.elpros.si/CDCheck/Help/crc.html – Visitado em abr/2006.

[RASH,2005] – RASH, Michael; OREBAUGH, Angela; CLARK, Graham; PINKARD, Becky; BABBIN, Jake. **Intrusion Prevention and Active Response**. Chapter 1 – Network Countermeasures – Rockland, United States of America – Syngress, 2005 página 7.

[REIS,2002] – REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Forense Computacional: Procedimentos e Padrões**. Capítulo 3 – Forense Computacional – Anais do IV Simpósio sobre Segurança em Informática 2002 – São José dos Campos, São Paulo, Brasil – página 102.

[SASHA,2003] – SASHA, **Holistic Approaches to Attack Detection**. Artigo do grupo Phrack Inc. – Volume 0x0b, Issue 0x39, Phile #0x0b of 0x12 – Disponível em: http://www.phrack.org/phrack/57/p57-0x0b – Visitado em mar/2006.

[SHOWSTUFF,2006] – How Stuff Works. **"Carnivore"** – Pesquisa no site How Stuff Works utilizando o termo "FBI Carnivore" – Disponível em: http://computer.howstuffworks.com/carnivore.htm – Visitado em abr/2006

[SILVEIRA,2005] – SILVEIRA, Enio Rovere; DANTAS, M.A.R. **Uma Abordagem de Monitoração de Tráfego de Rede utilizando Lógica Difusa**. Centro Tecnológico do Departamento de Informática e Estatística – Universidade Federal de Santa Catarina – Agosto 2005 – Disponível em: http://www.dcc.ufla.br/infocomp/artigos/v4.3/art05.pdf – Visitado em mar/2006.

[STANIFORD-CHEN,1998] – STANIFORD-CHEN, Stuart; TUNG, Brian; SCHNACKENBERG, Dan. **The Common Intrusion Detection Framework – CIDF**. Artigo aceito para o Workshop de Sobrevivência da Informação, Orlando, Flórida, Estados Unidos – Out. 1998. – Disponível em: http://www.isi.edu/gost/cidf/papers/cidf-isw.txt – Visitado em jan/2006.

[TANENBAUM,1997] – TANENBAUM, Andrew S. **Redes de Computadores**. Capítulo 1.4 – Modelos de Referência – 5ª Edição – Rio de Janeiro, Brasil – Campus, 1997 página 41.

[TAVARES,2002] – TAVARES, Dalton Matsuo. **Avaliação de Técnicas de Captura para Sistemas Detectores de Intrusão**. Capítulo 3.1.3 – Modelos Baseados em Análise – Tese apresentada para obtenção do Título de Mestre na Área de Ciências de Computação e Matemática Computacional –

Abr. 2002 – Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo – ICMC/USP – páginas 22-24.

[TERRA,2006] – Site Terra Educação. **Arquimedes** – Breve histórico sobre o físico, inventor Arquimedes no site Terra Educação – Disponível em: http://paginas.terra.com.br/educacao/fisicavirtual/grandes/arquimedes.htm – Visitado em mar/2006.

[TOXLAB,2006] – Birmingham Regional Laboratory for Toxicology – United Kingdom. **"Chain of Custody"** – Pesquisa utilizando o termo "Chain of Custody" – Disponível em: http://www.toxlab.co.uk/coc.htm – Visitado em abr/2006.

[UNIMAR,2000] – Apostila. **Sistemas de Banco de Dados** – Faculdade de Engenharia, Arquitetura e Tecnologia – Universidade de Marília, 2000. Disponível em: http://www.josevalter.com.br/download/banco_dados/BD1.pdf Visitado em mai/2006.

[WHATIS,2006] – What is. **"Network Forensics"** – Pesquisa no site What Is utilizando o termo "Network Forensicis" – Disponível em: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci859579,00.html – Visitado em abr/2006.

[WIKICHAIN,2006] – The Wikipedia. **"Chain of Custody"** – Pesquisa no wikipedia utilizando o termo "Chain of custody" – Disponível em: http://en.wikipedia.org/wiki/Chain_of_custody – Visitado em abr/2006.

[WIKICOMPFOR,2006] – The Wikipedia. "**Computer Forensics"** – Pesquisa no wikipedia utilizando o termo "Computer Forensics" – Disponível em: http://en.wikipedia.org/wiki/Computer_forensics – Visitado em mar/2006.

[WIKIFOR,2006] – The Wikipedia. **"Forensics"** – Pesquisa no wikipedia utilizando o termo "Forensicis" – Disponível em: http://en.wikipedia.org/wiki/Forensics – Visitado em mar/2006.

[WOOD,2006] – WOOD, Mark; ERLINGER, Michael. **Intrusion Detection Message Exchange Requirements**. – Draft do IDWG 2002 – Disponível em: http://www.ietf.org/internet-drafts/draft-ietf-idwg-requirements-10.txt – Visitado em fev/2006.

APÊNDICE E ANEXOS

APÊNDICE I

Questionário

Enviar por e-mail

Identificação: _____ Data: 12/06/06

Profissão: Cargo/função:

1) O que você, na execução de suas atividades, utiliza como fonte de informações para a análise forense de rede?

☐ *Logs* ☐ Cópia do Tráfego ☐ Outro: _____

2) Como você classificaria a credibilidade desta(s) fonte(s) de informações?

◯ Não-confiável ◯ Pouco conviável ◯ Confiável ◯ Muito conviável ◯ Completamente confiável

3) Qual a ferramenta você utiliza para busca e identificação de informações sobre ataques e atacantes recorrentes nos *logs*, base de dados ou em outras fonte de dados?

_____

_____

_____

4) Qual a técnica/ferramenta você utiliza para diferenciar acesso normal e eventos malignos dentro do universo de tráfego capturado em por um dispositivo de análise forense de rede?

_____

_____

_____

5) O tempo médio para a realização destas buscas é, na sua opinião:

◯ Muito lento ◯ Lento ◯ Moderado ◯ Rápido ◯ Muito rápido

6) Do universo de *logs* analisados, qual é o percentual que efetivamente faz referência a um ataque e serve como auxiliar na solução de um crime?

◯ 0 a 5% ◯ 5 a 25% ◯ 25 a 40% ◯ 40 a 60% ◯ 60 a 80% ◯ 80 a 90% ◯ 90 a 100%

7) Como você avaliaria o grau de consistência das informações disponibilizadas apenas por *logs*?

◯ Não-consistente ◯ Pouco consistente ◯ Consistente ◯ Muito consistente ◯ Completamente consistente

8) Como você avaliaria o grau de utilidade de uma ferramenta que filtrasse os *logs* e registrasse apenas os de tráfego malicioso?

◯ Extremamente útil ◯ Muito útil ◯ Útil ◯ Pouco útil ◯ Inútil

9) Como você avaliaria o grau de utilidade de uma ferramenta que fizesse um filtro e registrasse tanto os *logs* quanto cópia dos pacotes dos tráfegos maliciosos?

◯ Extremamente útil ◯ Muito útil ◯ Útil ◯ Pouco útil ◯ Inútil

10) Qual credibilidade você atribuiria a registros gerados por uma ferramenta analisasse o tráfego a procura de ataques, que quando percebesse ataques, efetuasse a cópia desse tráfego e o assinasse digitalmente armazenando a informação em um banco de dados?

◯ Não-confiável ◯ Pouco conviável ◯ Confiável ◯ Muito conviável ◯ Completamente confiável

ANEXO I

Markets, M-22-0693
R. Stiennon

Research Note
13 April 2004

Magic Quadrant for Intrusion Detection Systems, 2H03

The intrusion detection system market was marked by turmoil in 2003. Acquisitions and innovation have changed the vendor landscape. New technologies, such as intrusion prevention, are challenging traditional IDS products.

Core Topic
Security and Privacy: Security Infrastructure

Key Issue
Who are the leading providers of security infrastructure products and services, and what are their strategies, key offerings and business practices?

Strategic Planning Assumption
IDS vendors that have not introduced blocking capabilities by the end of 2004 will not be viable providers beyond the end of 2005 (0.9 probability).

The intrusion detection system (IDS) industry is struggling to justify inordinate investments in complicated, expensive technology that does little to protect the enterprise. Because IDS has reached the peak of its usefulness as a stand-alone technology, and intrusion prevention system technologies are offering significant challenges to IDSs, this will be the final IDS Magic Quadrant that Gartner presents.

Signature-based inspection is a subset of features that can be found in intrusion prevention systems and next-generation firewalls. Many traditional IDS vendors will develop in-line blocking solutions as they migrate to intrusion prevention. In doing so, they must contend with the visionaries that are leading this area. They also must inspect traffic at multiple gigabit speeds, while introducing minimal network latency. IDS vendors that have not introduced blocking capabilities by the end of 2004 will not be viable providers beyond the end of 2005 (0.9 probability).

Investments in security technology should lead to enhanced security. IDS products don't fit this criterion. By contrast, vulnerability management, patch management, network segmentation, network and host intrusion prevention, firewalls and antivirus products contribute to a more-secure enterprise. Although these technologies must detect, then block, attacks, their value is in the blocking, not the detection. Enterprises should invest in these technologies, and only then consider an alerting capability such as an IDS that can assist in the forensics task of tracking down and repairing damage from successful attacks.

IDSs must move toward monitoring and alerting on the misuse of IT resources by authenticated, authorized users. This means evolving up the stack to the application layer. However, the

network-and syslog-based IDS technologies that are represented in this Magic Quadrant don't lend themselves to the detection of business-layer offenses. Thus, other vendors likely will address these needs. For example, Covelight Systems, Vericept and Oversight Technologies are bringing such products to market.

Changes that occurred in the IDS vendor landscape in 2003 include:

- Symantec purchased startup Recourse Technologies.
- Cisco Systems terminated its relationship with Entercept Security Technologies to purchase Okena, a desktop and server intrusion prevention vendor.
- Network Associates acquired Entercept and IntruVert.
- NFR Security, after acquiring the Centrax host-based intrusion detection technology from CyberSafe, hired new management and discontinued the Centrax host protection products.
- Enterasys Networks settled an investigation by the U.S. Securities and Exchange Commission (SEC) and moved forward with its Secure Networks solution.
- Internet Security Systems (ISS) introduced its Proventia line of defense products.

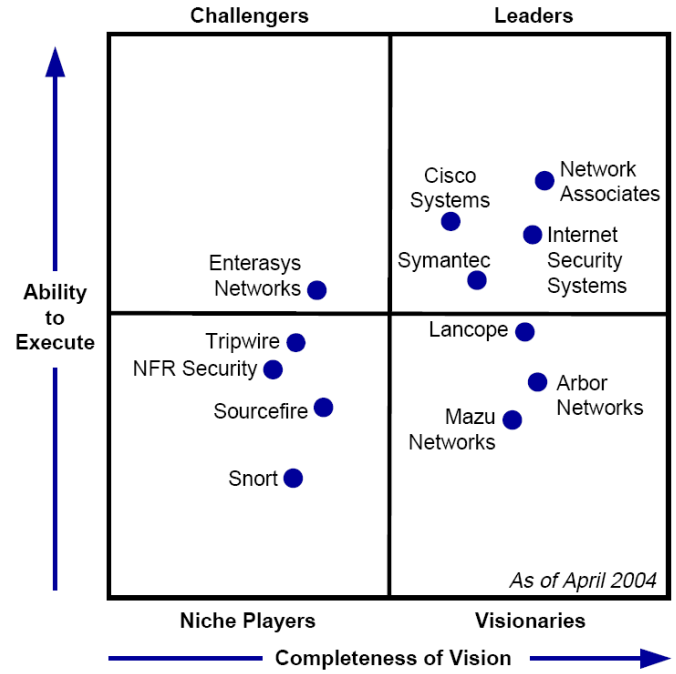
Several vendors on the IDS Magic Quadrant have good network and event analysis capabilities that give them higher rankings, such as Arbor Networks and Lancope.

Pure-play intrusion prevention vendors, such as Radware, Reflex Security, TippingPoint Technologies and TopLayer Networks, are not included on the IDS Magic Quadrant. They will be discussed in upcoming Gartner research.

Evaluation Criteria and the Magic Quadrant

The IDS Magic Quadrant (see Figure 1) is a graphical portrayal of vendor performance and capability in the IDS market segment, based on viability, service/support, features and functionality, and technology.

Figure 1
Magic Quadrant for Intrusion Detection Systems, 2H03



Source: Gartner Research (April 2004)

"Ability to Execute" shows Gartner's view of how well a vendor is positioned to gain market share or deliver on its promises. Key execution criteria for the IDS market include a vendor's distribution channels, financial parameters, and the reputation of its management/technical team and support. Acquisition by a financially viable vendor, such as Cisco or Network Associates, usually is a significant benefit.

"Completeness of Vision" is Gartner's view of how well a vendor anticipates or leads evolving enterprise demands for better security tools that add, at least incrementally, to an enterprise's overall security posture, based on input from Gartner clients.

Magic Quadrants provide an understanding of vendor positioning and set performance expectations for vendors. Appropriate vendors can be found in all quadrants, not only among market leaders. Some vendors may be appropriate for only certain vertical markets.

Leaders

Cisco Systems ended its partnership with Entercept to purchase Okena, a host intrusion prevention vendor. Although Cisco is not positioned as a security software vendor, the Okena solution

offers better security value than traditional host-based IDS products. In the wake of the MSBlast worm, many enterprises are looking to protect internal desktops. The Cisco Security Agent is one of the few contenders for that application. In addition, Cisco is negotiating the purchase of Riverhead Networks. This could signal an intrusion prevention strategy for Cisco, although it will be late to market.

ISS's RealSecure line of network and host IDS sensors is the most-deployed IDS solution in the market. RealSecure 7.0 has reduced false-positive rates by an order of magnitude. Even in the typical range of several thousand alerts a day, this is still too "noisy" to offer real value in detecting and responding to attacks. ISS has maintained a position in the Leaders quadrant by taking dramatic steps to reinvent itself around its Proventia line of products. Because in-line security devices must have low latency and run at wire speeds, hardware-based vendors will challenge software solutions that run on dedicated appliances. The RealSecure Server product line has incorporated protection capabilities from ISS's BlackIce product acquisition; thus, it also qualifies as a host intrusion prevention product.

In 2003, **Network Associates** acquired Entercept and IntruVert, which were early innovators in the intrusion prevention area. We believe that a desktop antivirus vendor such as Network Associates (McAfee) should be in the host protection business. The acquisition of Entercept is a strong addition to other McAfee products. IntruVert took one of the "Four Paths to True Network Security" — IDS — and gained more traction with that message than other intrusion prevention vendors. IntruVert is winning deals against traditional IDS vendors, and many customers are turning on its blocking functionality in their in-line devices. The combination of a host and network strategy for technology that goes beyond alerting to blocking has earned Network Associates a leader position in the IDS Magic Quadrant. Its major challenge is to execute rapidly on a combined desktop security agent with seamless management integration to IntruShield-based network protection.

Symantec acquired Recourse Technologies, whose network IDS sensor uses flow-based threat identification to more-reliably detect network abuse. Symantec gets high points for improving on IDS technology. However, the lack of a host and network protection strategy will keep Symantec from gaining rapid penetration into the enterprise. Its direction on managed services and enterprise security management is in opposition to its stated desire to lead in network security products.

Challengers

Enterasys Networks overcame its financial reporting issues and SEC challenges in 2003. While its focus was on the SEC investigation, Enterasys missed the shift in security technology from noisy IDS sensors toward enterprise protection. It has refocused its marketing message around its Secure Networks solution, and is emphasizing how IDS can work with its other LAN solutions to counter attacks from worms and internal threats. These are good messages, but Enterasys has not demonstrated the product innovation to lead in this area.

Visionaries

Arbor Networks is not technically an IDS vendor. However, its PeakFlow X line of network sensors provides a rich understanding of network traffic, protocol usage and anomalous behavior. Triggers can be set that enable the device to communicate to edge routers, and rate-limit or block certain types of traffic. This is an effective tool during virus and worm outbreaks. Arbor Networks enables enhanced knowledge of network usage, which is a strong value proposition for enterprises.

Lancope's StealthWatch is a network traffic anomaly tracking tool, similar to PeakFlow X. Lancope gets high vision marks for this approach, because tracking usage and network debugging is one of the most-valuable features of IDSs.

Mazu Networks uses flow data to map normal behavior and present it in a graphical format that assists in debugging network issues. Mazu's Profiler product line provides the type of network usage visibility that signature-based IDSs can't do well.

Niche Players

NFR Security has brought in new top management (again) and has refocused on its network IDS product. Its Centrax acquisition, which was supposed to give NFR an endpoint security marketing strategy, has been discontinued. Its focus on intrusion management as a way to better detect intrusions only highlights the primary deficit with IDSs — that is, that they detect, but do not block, intrusions.

Snort is the first open-source solution to be placed on the IDS Magic Quadrant. Snort (available for download at www.snort.org) has become a standard in intrusion detection. Many vendors use Snort signature definitions in their products. All security event management consoles accept alerts from Snort sensors, and managed security service providers include Snort in their low-cost sensor appliances (see "Magic Quadrant for North American MSSPs, 1H03"). Enterprises that have not selected a network IDS product should install Snort sensors to gain experience with

IDS before committing additional resources.

Sourcefire is a commercially supported version of Snort that was founded by Snort's creators. Significant venture funding and first-year revenue indicate that there is strong demand for low-cost IDS appliances. Sourcefire's best product offerings are in the real-time network awareness area. The Sourcefire Real-time Network Awareness product combines vulnerability scanning, network discovery and alerting — a valuable departure from signature-based IDSs.

Tripwire offers a popular host-based IDS solution that uses file-integrity checking to provide point-in-time assurance that an attack has not succeeded. Conversely, it can help identify compromised machines during the remediation process after a successful attack. Tripwire is moving from an IDS strategy to a system configuration enforcement model.

Bottom Line: Technologies have emerged that enhance network security by enabling enterprises to block attacks to protect their networks and IT resources. Firewalls, vulnerability management and intrusion prevention systems counter threats posed by worms, increased hacking activity and enterprise insiders. As enterprises scrutinize IT budgets, they should curtail spending on intrusion detection system tools, as well as the people and systems to monitor them, in favor of spending for blocking and prevention technologies.

Magic Quadrant for Network Intrusion Prevention System Appliances, 2H05

30 November 2005

Greg Young John Pescatore

Source: Gartner
Note Number: G00133189

The network intrusion prevention system appliance market is in a period of maturity and consolidation. A smaller group of vendors are getting an increasing percentage of the market, but the evolving threat means that those that fail to maintain innovation ahead of market demands will be left behind.

What You Need to Know

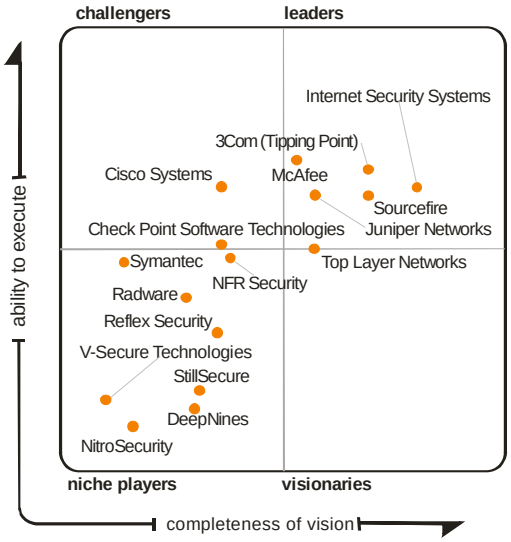
Network intrusion prevention system (IPS) can detect and block attacks, such as worms, and act as a pre-patch shield for systems and applications. The Sasser and Zotob worms have driven network IPS to be ready for enterprise use. The market for network IPS appliances is entering a phase of maturity and consolidation. The significant benefits of an in-line attack-blocking technology can only be realized with a product that fits your security processes and is sized appropriately. The Magic Quadrant for Network Intrusion Prevention System Appliances is illustrated in Figure 1.

Strategic Planning Assumption(s)

Sales of stand-alone IPS appliances will be less than 10 percent of overall next-generation firewall revenue by the end of 2008 (0.7 probability). Through 2007, in-house testing will have been done for 90 percent of new acquisitions of network IPS in appliances and next-generation firewalls (0.8 probability).

Magic Quadrant

Figure 1.
Magic Quadrant for Network Intrusion Prevention Systems Appliances, 1H05



Source: Gartner (November 2005)

Market Overview

The network IPS market has its roots in the improvement and often replacement of intrusion detection systems (IDSs). IPS contains all the detection features of IDS, with two critical areas of improvement: (1) Intrusion prevention moves beyond simple attack signature detection to add vulnerability-based signatures as well as anomaly detection capabilities; and (2) network IPS sensors have high processing rates to support in-line automated blocking or handling of attacks. Essentially, network IPS adds "block attacks and let everything else through" security enforcement to the "deny everything except that what is explicitly allowed" policy enforcement provided by the first generation of firewalls. By

the end of 2006, most next-generation firewalls will likely use common processing engines to support both functions in one product.

The network IPS market for stand-alone appliances was approximately $246 million in 2004 (including product and maintenance but not services) and will increase to more than $400 million by the end of 2005. McAfee had the largest IPS market share of revenue, followed closely by TippingPoint and Internet Security Systems (ISS). This is a crowded market with several dozen vendors providing network IPS products, many with very small installed bases. Consolidation will likely continue because there already is increasing consistency of shortlists of vendors, particularly in larger enterprises. For more on this subject, see "The Network IPS Market Will Consolidate in 2005."

Vendor lineage is stereotyped in the products: IPS from security companies tends to be strong on security function and less impressive on network performance, which is the opposite of companies in which security is not their primary business (for example, network infrastructure vendors and startups). These differences will be reduced in the midterm and, in the long term, will become almost irrelevant as the next-generation firewall market increases (see "Network Security Platforms Evolving Into Single-Appliance Solutions.")

On average, solutions are priced to $50,000 per Gbps of deep inspection (this is an average, and many products provide less than 1-Gbps capability). Most vendors provide more than five models, with some entry-level products offered for less than $15,000. Maintenance fees vary considerably. Signature update fees also vary but are included with maintenance for most products. Most products include a local-management console, with dedicated management appliances resulting in an additional cost. The total cost of ownership and system management capabilities of network IPS products should be key evaluation criteria when comparing competing products.

Reliability and availability are also key criteria for any in-line device. Bypass unit modules allowing fail-open for copper ports are an additional charge for Reflex, Radware (except the DefensePro 3020), and Check Point Software Technologies (for the 410 and 610 products only). With other vendors, this is included in the base price for units in recognition that this is the standard deployment mode for most.

Market Definition/Description

The network IPS market includes in-line devices that perform full-stream assembly of network traffic, and they provide detection, using several methods including signatures, protocol anomaly detection, and behavioral or other techniques.

Network IPS is also provided within a next-generation firewall, which is the integration of an enterprise-class network firewall and network IPS. The next-generation firewall market will subsume the stand-alone network IPS appliance market (which is the subject of this Magic Quadrant) at the enterprise edge. However, this will not occur immediately because of the following factors:

- Enterprise firewall vendors have been slow to imbue the IPS within their next-generation firewall products with the same capabilities as the stand-alone appliances they offer.
- The firewall refresh cycle for the enterprise is between three and five years, meaning many enterprises will not look at the next-generation firewall to replace established firewalls until as late as 2009.
- New network security technologies are often provided first through separate appliances before being included in other offerings.

The network IPS market is already in the first stage of consolidation, with Gartner seeing a more consistent list of vendors on our customers' shortlists. With fewer companies receiving a larger share of the revenue, there are opportunities for the acquisition of companies providing quality products, but there are risks for buyers of products if the buyers are not increasing their installed base.

Inclusion and Exclusion Criteria

Only products that met the following criteria were included:

- Products that meet Gartner's definition of network IPS
- Operate as an in-line network device that runs at wire speeds
- Perform packet normalization, assembly and inspection
- Apply rules based on several methodologies to packet streams, including (at a minimum) protocol anomaly analysis, signature analysis and behavior analysis
- Drop malicious sessions — do not simply reset connections
- Achieved IPS product sales in the last year of more than $1 million within a customer segment that is visible (for example, a single sale of $1 million would not be considered)

- Products and vendors were excluded if:
- They provide only a next-generation firewall platform, which is covered in "Magic Quadrant for Network Firewalls, 2H04." We should note that next-generation firewall vendors, which provide an IPS appliance, have that appliance included in this Magic Quadrant (Juniper ISG and Check Point with SmartDefense firewalls).
- They are in other product classes or markets, such as:
- Network behavior anomaly detection products. Products from companies such as Arbor Networks, Lancope, Mazu Networks and Q1 Labs. These products are not in-line IPS, but instead focus on networkwide detection of anomalies and provide only reactive capabilities, such as modifying access control lists. IPS vendors are beginning to implement feeds from network anomaly detection as one means of having intelligence from across the network, which can be used to prioritize blocking.
- Network access control (NAC) products are not IPSs and are covered in other Gartner research. NAC focuses on quarantining authorized endpoints that are infected or vulnerable, rather than actively shielding against attacks.
- Are host IPSs. Software is on servers and workstations rather than an in-line device on the network.

Evaluation Criteria

Ability to Execute

The Ability to Execute criteria include:

- Product service and customer satisfaction in deployments
- Overall business viability, including overall financial health and prospects for continuing operations
- Sales execution and pricing including dollars per Gbps, revenue, average deal size, installed base and use by managed security service providers (MSSPs)
- Market responsiveness and track record. Delivering on new features, such as receiving and acting on feeds from outside the IPS, rate shaping and quality of service, and solid multi-device management.
- Market execution, including delivering on features and performance, such as product vision, customer satisfaction with those features, and those features winning out over competitors in selections. Delivering products, which are low latency and multi-Gbps, have solid internal security, behave well under attack, have high availability, and are available ports that meet demands, is rated highly. Speed of vulnerability-based signature production was highly rated.
- Customer experience and operations, including management experience and track record, and depth of staff experience, specifically in the security marketplace. Also important is low latency, rapid signature updates, overall low false positive and negative rates, and how the product fared in events such as the Zotob and Slammer worms.

Table 1.
Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	standard
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	standard
Marketing Execution	standard
Customer Experience	standard
Operations	standard

Source: Gartner

Completeness of Vision

The Completeness of Vision criteria include:

- Market understanding and strategy. This includes providing the correct blend of detection and blocking technologies that meet the requirements for IPS, innovation, having

vulnerability rather than exploit product focus, and integration with other security solutions. Also included is understanding and commitment to the security market and, more specifically, the network security market. Vendors that rely on third-party sources for signatures or have weak or "short cut" detection technologies score lower.

- Sales strategy includes pre- and post-product support, value for pricing, and providing clear explanations and recommendations for detection events.
- Offering strategy, with emphasis on product road map, signature quality, next-generation firewall integration and performance. Successfully completing third-party testing, such as the NSS Group IPS tests and Common Criteria evaluations, is important. Vendors that reissue signatures, are overreliant on behavioral detection and are slow to issue quality signatures do not score well.
- The business model includes the process and success rate for developing new features and innovation and R&D spending.
- Vertical, industry and geographic strategy includes the ability and commitment to service geographies and vertical markets (for example, MSSP and the financial sector).
- Innovation, including R&D, and quality differentiators, such as performance, management interface and clarity of reporting. The road map should include moving IPS into new placement points and better-performing devices.

Table 2.
Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	standard
Offering (Product) Strategy	standard
Business Model	standard
Vertical/Industry Strategy	low
Innovation	standard
Geographic Strategy	low

Source: Gartner

Leaders

Leaders demonstrate balanced progress and effort on all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain in the Leaders quadrant, these vendors must have demonstrated a track record of delivering successfully in enterprise IPS deployments and winning in competitive assessments. Leaders produce products that provide high signature quality, offer low latency, and have a range of models. Leaders consistently win selections and have been consistently visible on enterprise shortlists.

A leading vendor is not a default choice for every buyer, and clients are warned not to assume that they should buy only from the Leaders quadrant.

Challengers

Challengers have products that address the typical needs of the market with strong sales, visibility and clout that add up to higher execution than niche players. Challengers often succeed in established customer bases but do not yet fare well in competitive selections.

Visionaries

Visionaries invest in the leading/bleeding edge features that will be significant in next generation of products and give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution skills to outmaneuver challengers and leaders. There are currently no IPS vendors that meet these criteria.

Niche Players

Niche players offer viable solutions that meet the needs of some buyers. Niche players are less likely to appear on shortlists, but they fare well when given the right opportunity. While they generally lack the clout to change the course of the market, they should not be regarded as merely following the leaders. Niche players may address subsets of the overall market (for example, the small and midsize

business [SMB] segment or a vertical market), and often they can do so more efficiently than the leaders. Niche players are often smaller firms, produce only software appliances, and/or do not yet have the resources to meet all of the enterprise requirements.

Vendor Comments

3Com (TippingPoint)

Acquired by 3Com earlier this year, TippingPoint did not suffer any significant drop in performance from this change. As a pure-play IPS vendor and not having to convert an IDS product, TippingPoint had the advantage of designing its products to perform well in a network environment. With a 5-Gbps product, TippingPoint devices have been shown to be well-behaved in-line devices and often win product selections in which low latency is heavily weighted.

If 3Com executes correctly, TippingPoint will be able to move IPS onto a switch and also utilize 3Com channels for the SMB market when they introduce sub-11-Mbps products. 3Com showed its commitment to advancing IPS as a key product area by appointing Tippingpoint's CTO as the 3Com CTO. TippingPoint does not offer a network firewall on its IPS and will need to do so in order to enter the next-generation firewall market.

Check Point Software Technologies

Check Point Software Technologies has not had a stand-alone IPS appliance for the enterprise edge. Check Point does provide a next-generation firewall in its Smart Defense offering, but it really has not had a purpose-built in-line sensor offering. Check Point InterSpect is its "internal IPS" offering, but this has had limited visibility in the network IPS appliance space, which is driven by edge requirements. To remedy this, Check Point announced its intention to acquire Sourcefire (the acquisition will be completed in the first quarter of 2006). This has the potential to provide a stronger deep-inspection engine across the Check Point platforms, particularly if Check Point integrates SourceFire RNA across its products. Check Point is financially strong, and its wide international support is important for deployments across the world.

Cisco Systems

Cisco Systems entered the IPS space this year with an offering across an impressive number of platforms. In addition to the IPS appliance, Cisco IPS software can also be run on IOS platforms, on ISR routers, on IDS/IPS blades in Cisco switches, within the ASA appliance, on access routers and on PIX firewalls.

Cisco's IPS appliance is its former IDS platform with the software upgraded and reconfigured for placement in-line. Enterprises that are nearly "all Cisco" in infrastructure are good candidates for Cisco IPS, especially enterprises in which Cisco IDS is already in place. With the IPS products less than 1 year old, Cisco is not often winning in competitive product selections against other IPS.

DeepNines

DeepNines has pursued the "far edge" placement point with IPS offering a Layer 2 transparent (no IP address) in-front-of-the-router device. DeepNines expanded this line to include traditional IPS, which can be applied to a wider number of placement points. These software appliances are close in functionality to an all-in-one appliance and may be attractive to the SMB market because they include a firewall, gateway antivirus and some anti-spyware capability.

Internet Security Systems

A security company with a strong history in IDS, Internet Security Systems has two significant assets outside its IPS appliance: its X-Force vulnerability research team and its MSSP business. Investing in vulnerability research has allowed ISS to be the leader in new signatures, and this capability has driven its product design around vulnerabilities rather than exploits, which is fundamental to good-performing IPS and sound signatures. ISS design investments in IPS have made it easier for it to add new protocols (for example, voice over Internet Protocol [VOIP]), for inspection within its Protocol Analysis Module (PAM). ISS has been successful in migrating its IDS customers to the Proventia G, but it is held back from greater success by not yet offering a high-performance purpose-built appliance. IPS management is integrated with other ISS products via the SiteProtector manager.

Juniper Networks

Netscreen was an early innovator with deep-packet inspection after its acquisition of OneSecure. With the Juniper acquisition now behind it, innovation and new product features are again showing up in its IPS products, with full-featured appliances up to 1 Gbps inspecting a large number of protocols. As with its firewall competitor Check Point, Juniper is well-positioned in the next-generation firewall market (the hardware-based ISG firewalls provide up to 2 Gbps of deep inspection), yet Juniper has

not maintained high visibility in the IPS appliance space with its IDP IPS products. Juniper's software-based hardware IDP IPS appliance is popular with enterprises that already own Juniper infrastructure equipment. The Juniper IDP product has a range of models and a strong management console.

McAfee

McAfee, known more for antivirus software rather than network security, has had considerable success in the IPS field through acquisition and enhancement of the IntruShield product. McAfee is often seen on enterprise IPS short lists with its purpose-built IntruShield IPS and performs well in throughput testing. IntruShield includes Secure Sockets Layer (SSL) acceleration/inspection technology and has a 2-Gbps appliance. McAfee has been including customization for MSSPs in recognition of the growing market for customer premises and "in the cloud" managed services. For more information on this subject, see "'In the Cloud' Security Services Will Change Providers' Landscape."

To maintain this lead, McAfee must incorporate a strong network firewall with its IPS (for example, a next-generation firewall), and integrate IntruShield with its other products through a unifying management console capability.

NFR Security

NFR Security has leveraged its IDS lineage to move into the IPS space with its Sentivist product line. Although Sentivist IPS is a software appliance, NFR is seeing success at the enterprise and with the government deployments. With a separate management appliance as a mandatory, NFR is better suited to multiappliance deployments. Sentivist offers a good interface, good reporting, a minimum of configuration and is suited for sub-200-Mbps placement points. NFR recently released an Enterprise Series Sensor line for higher throughput placement points.

NitroSecurity

NitroSecurity takes a nontraditional approach to IPS with an emphasis on the custom database within its software appliance IPS and detection weighted toward correlation and quarantine rather than signatures. NitroSecurity offers a Layer 2 transparent mode IPS that is seeing success in healthcare and education verticals. NitroSecurity proposes some innovative features on its IPS road map but requires increased signature emphasis, better support and financial strength to move up to competing effectively in enterprise shortlists.

Radware

Radware offers purpose-built multigigabit IPS appliances up to 3 Gbps. Capitalizing on its network expertise, Radware DefensePro IPS includes solid in-line behavior, such as low latency and denial of service (DOS) features, including traffic shaping. Radware has increased its investment in vulnerability and IPS signature research but lags the leaders in proactive protection.

Reflex Security

Reflex Security is a startup IPS firm offering a low-cost software appliance requiring a minimum of configuration designed for SMBs and Type C enterprises and the MSSPs servicing them. The Reflex product overlaps the all-in-one security appliance space as it includes firewall, gateway antivirus and anti-spyware; however, it is most often deployed for its IPS capabilities.

Sourcefire

Sourcefire has leveraged its IDS lineage successfully into IPS. Sourcefire developed a purpose-built appliance this year, allowing it to compete more effectively at the enterprise.

Sourcefire IPS can now receive feeds from the Sourcefire RNA vulnerability assessment product to allow the IPS to make prioritized blocking decisions and have endpoint (clients and servers) visibility (see "Use Endpoint Intelligence to Improve Security Defenses". Although Sourcefire manages the open-source Snort IDS product, its IPS is full-featured and is not to be confused with in-line original equipment manufacturer (OEM) Snort implementations. Sourcefire IPS is also available via OEM through Nortel Networks and on the Crossbeam platform. Check Point announced it would be completing proposed acquisition of Sourcefire in the first quarter of 2006.

StillSecure

Strata Guard (renamed from BorderGuard) is a software appliance solution suited to sub-Gbps placement points. BorderGuard IPS is integrated with the StillSecure VAM vulnerability management product supporting the reality that IPS is part of a process of vulnerability remediation (see "Intrusion Prevention Process Consists of Seven Steps". Having the vulnerability management feed widens the network view for more-intelligent IPS alerting and blocking decisions.

Symantec

Symantec's SNS 7000 series appliance has low visibility in the enterprise market, but this is consistent with Symantec's focus on the SMB multifunction network security appliance space, and that the product is very new to the market. The SNS is friendly for administrators, uses the familiar LiveUpdate for signature updates, has clear incident viewing, and includes innovative elements, such as FlowChaser, which allows for identifying the source of DOS attacks. SNS has not done well in competitive IPS "bake-offs," primarily from a network performance perspective, but it is popular with enterprises that have a large Symantec investment.

Top Layer Networks

Top Layer Networks' lineage is load balancing and edge-of-network DOS. This has translated well to IPS, with Top Layer offering purpose-built hardware in the multi-Gbps placement points with its 5500 appliance. Top Layer provides a balanced blend of safeguards and detection methods, including network firewall, DOS protection and traffic shaping. Top Layer lags other players in the proactive protection of narrow blocking signatures, but it does have multidevice management capabilities, low latency and good post-sales support.

V-Secure Technologies

V-Secure takes the approach that is weighted heavily toward behavioral detection in its software appliance. Signature detection was introduced in version 8.0 in recognition that signatures are a required detection technology. V-Secure signature release times are longer than the industry average.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.
Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.
Business Model: The soundness and logic of the vendor's underlying business proposition.
Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.
Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.
Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.
