Tecnologias de Sistemas de Detecção e Prevenção de Intrusão (IDP) aplicados em ambientes de rede de dados híbridas: avaliação das necessidades e seleção das ferramentas

Elvis Pontes

OBJETIVO

Este artigo tem como objetivo prover procedimentos e uma breve metodologia estruturada, mas flexível, para a seleção, especificação, avaliação, implementação E configuração de tecnologias de sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS) e sistemas de detecção e prevenção (IDP) para proteção de sistemas de informação e redes de dados. Procura-se, neste artigo, caracterizar sumariamente as quatro principais classes de produtos IDP: produtos baseados em rede, baseados em rede sem fio, softwares de detecção de comportamento anômalo de rede, e baseados em *host*. Procura-se também caracterizar o ambiente mais propício para aplicação de cada classe de produto IDP. Para consecução deste artigo, desenvolveu-se uma pesquisa identificando os tipos de tecnologias disponíveis, o escopo de aplicação e as potencialidades das mesmas, de forma a se estabelecer dentro da análise as tecnologias mais aplicáveis ao ambiente estudado, para satisfazer a necessidade de controle específico na mitigação eficiente e eficaz do risco determinado, em alinhamento com a política de segurança estabelecida.

RESUMO

Para que se efetue adequadamente a avaliação de produtos IDP, há a necessidade, em primeira mão, de serem definidos os perímetros do ambiente e os requerimentos genéricos que estes produtos devem compreender. As características e metodologias de produtos IDP são consideravelmente diversas. Portanto, uma boa solução de IDP implementada em uma organização talvez não seja ideal e nem satisfaça os requerimentos de uma outra. A principio, recomenda-se que as características dos sistemas da organização e, principalmente, do ambiente da rede de dados precisam ser devidamente analisadas, assim um produto IDP pode ser selecionado de forma mais alinhada com os requisitos e consequentemente monitorar os eventos de interesse dos sistemas e/ou da rede. É recomendável também que a mesma metodologia seja adotada no desenvolvimento de soluções IDP. Após a análise dos sistemas e ambiente de rede de dados, há de se definir os objetivos e metas que se desejam alcançar na aplicação da solução IDP. As políticas de segurança existentes no ambiente organizacional devem ser revistas e analisadas antes da etapa de seleção dos produtos, pois estas servem como especificação para muitas características que devam ser cobertas pelo produto IDP. Há ainda de se acrescentar a possibilidade de processos de auditoria, que podem ou não ser instituídos.

INTRODUÇÃO

Detecção de intrusão é o processo de monitoramento e análise de eventos que ocorrem em um sistema de computadores ou em uma rede de dados, em busca de sinais de incidentes em potencial, os quais podem ser violações ou ameaças iminentes de violação das políticas de segurança.

Prevenção de intrusão é o processo da realização da detecção de intrusão no esforço de deter incidentes em potencial detectados.

Sistemas de detecção e prevenção (IDPs) estão focados na identificação de incidentes em potencial, controle de logs dos mesmos, no combate aos incidentes e em reportá-los aos administradores de segurança. Adicionalmente, as organizações usam IDPs para outros propósitos, como na identificação de problemas com políticas de segurança, na documentação de ameaças existentes, e na dissuasão de funcionários, terceirizados, prestadores de serviço ou quaisquer indivíduos que violem a política de segurança. IDPs tornaram-se uma necessidade adicional a infra-estrutura de segurança da maioria das grandes corporações.

IDPs gravam informações relacionadas a eventos observados, notificando e reportando administradores de eventos importantes. Muitos IDPs podem também responder a uma ameaça detectada no esforço de prevenir a mesma de explorar a vulnerabilidade do sistema. Utilizam-se várias técnicas de resposta, que permitem ao IDP combater o ataque por si só, alterando o ambiente de segurança (reconfigurando o Firewall p. ex.), ou alterando o conteúdo do ataque.

Existem muitos tipos de tecnologias IDP, as quais são diferenciadas principalmente pelos tipos de eventos que as mesmas podem monitorar e as formas que são empregadas. Serão apresentados e discutidos quatro tipos de tecnologias IDP:

- Baseado em rede – monitora o trafego de rede para dispositivos ou seguimentos de rede em particular e analisa a rede e a atividade de protocolos de aplicação para identificar atividade maliciosa;
- Baseado em redes sem fio – monitora o tráfego de rede sem fio e o analisa para identificar atividade maliciosa e suspeita que envolva o próprio protocolo de rede sem fio.
- Detecção de comportamento anômalo de rede – examina o trafego de rede para identificar ameaças que gerem um trafego de rede anormal, como ataques DDoS, escaneamento de portas e alguns tipos de malware.
- Baseado em Host – monitora as características de um único host e os eventos que ocorrem no mesmo de forma suspeita.

A proteção dos componentes IDP é essencial para integridade dos mesmos, já que estes são alvos de ataques que visam danificá-los de forma a barrar detecções, ou ataques que visam obter acesso a informações privilegiadas, como configurações de hosts. Os IDPs são compostos de diversos componentes, incluindo sensores e agentes, servidores de gerenciamento, servidores de dados e, usuários e consoles para administração. Todos os componentes de operação e aplicações devem ser bem guardados e mantidos atualizados.

Ações específicas de proteção incluem contas separadas para cada usuário IDP e para o administrador, restrição e segregação de rede para melhor controle de acesso aos componentes IDP e garantir que as comunicações com o gerenciador IDP estão protegidas adequadamente (criptografia de dados ou transmissão dos dados em rede segregada).

Os administradores devem manter a segurança dos componentes IDP de forma contínua, já que novas ameaças surgem todos os dias. A verificação de funcionalidade de todos os componentes é um ponto importante: monitoramento dos componentes quanto detalhes de segurança, realização de testes de vulnerabilidade periódicos, verificação das respostas à exploração de vulnerabilidades, atualização e testes de atualização.

Outro ponto importante é a realização de *back up*s regulares das diversas configurações de todos os recursos IDP, conforme o preconizado nas políticas de segurança.

A utilização de tecnologias diversas de IDP deve ser considerada para alcançar uma maior acuidade na detecção e prevenção de atividades maliciosas.

Os tipos primários de tecnologias IDP oferecem recursos diferentes para ordenação de informação, registro de *logs*, detecção e prevenção. Cada tipo de tecnologia tem vantagens sobre a outra, como detecção de alguns eventos que outras não realizam e detecção de alguns eventos com maior exatidão que a outra. Em muitos ambientes, uma solução robusta de IDP não pode ser alcançada sem a utilização de vários tipos de tecnologias IDP. Para a maioria dos ambientes, uma combinação de tecnologias como a baseada em rede e a baseada em *host* é necessária para a solução eficiente e efetiva do IDP.

Tecnologias IDP sem fio também pode ser necessárias se a organização quiser garantir que as mesmas precisam de proteção e monitoramento adicional. Tecnologias de detecção de comportamento anômalo de rede (NBAD – Network Behavior Anomaly Detection) podem também ser implementadas se a organização desejar recursos de proteção adicional para ataques de negação de serviços, worms, e outras ameaças que os NBAD estão preparados para detectar.

Organizações que planejam usar múltiplos tipos de tecnologias IDP ou múltiplos produtos da mesma tecnologia IDP, deveriam considerar os pontos de integração destas tecnologias (ou a inexistência destes pontos).

A integração IDP é freqüentemente realizada quando uma organização utiliza vários produtos IDP de um único vendor, por ter um único console que pode ser usado no gerenciamento e monitoramento de múltiplos produtos.

Alguns produtos podem também compartilhar dados, o que aumenta a velocidade de análise e ajuda aos usuários a melhor priorizar as ameaças. Uma forma mais limitada da integração direta é o uso de produtos IDP que fornece dados para outro.

Integração indireta de IDPs são realizadas por softwares de segurança de informação e gerenciamento de eventos (SIEM – Security Information and Event Management), que são desenvolvidos para importar informações de vários logs de segurança relacionados, bem como efetuar a correlação de eventos entre os mesmos. Softwares SIEM complementam os IDPs de formas diversas, incluindo a correlação de eventos por diferentes tecnologias, visualização de dados de várias fontes de eventos e provendo informação de suporte para outras fontes, ajudando os usuários a determinar a exatidão dos alertas IDP.

Antes de avaliar os produtos IDP, as organizações deveriam definir os requisitos dos produtos devem satisfazer. Os técnicos que efetuam a avaliação precisam entender as características do sistema organizacional e ambientes de rede, então um IDP pode ser

selecionado de forma a ser compatível com estes requisitos, tornando-se, assim, pronto para efetuar monitoramento dos eventos de interesse nos sistemas e/ou redes.

Os objetivos e metas devem ser articulados, de forma a serem alcançados pelo uso de um IDP, como a detecção e prevenção de ataques comuns, identificação de erros de configuração de dispositivos de rede sem fio, e detecção de uso incorreto dos sistemas e recursos de rede das organizações. Devem também ser revistas as políticas de segurança existentes, as quais servem como especificação básica para muitos dos recursos que os produtos IDP devem prover. Adicionalmente, deve-se analisar os pontos de auditoria externas, bem como a necessidade de produtos específicos para satisfazer essa necessidade, ou não.

Deve-se levar em consideração as restrições de recursos. Deve-se, ainda, considerar a necessidade de definição dos seguintes grupos de requisitos:

- Condições de segurança – incluindo coleta de dados, registro de log, detecção e prevenção;
- Performance – incluindo capacidade máxima e dispositivos para mensuração de performance;
- Gerenciamento – incluindo projeto e implementação, operação e manutenção (software updates), treinamento, documentação e suporte técnico;
- Ciclo e vida e custos.

Durante a fase de avaliação de produtos IDP, as organizações devem considerar o uso da combinação de várias fontes de dados, nas características de recursos dos produtos.

Fontes de dados comuns desse produtos incluem testes de laboratório ou testes de aplicações reais, informação fornecida pelo vender, revisões de terceiros e/ou experiência por outros profissionais dentro da organização ou recomendações de outras organizações. Quando do uso de dados por outras partes, organizações devem considerar se as mesmas são fidedignas,

Infelizmente IDPs não fornecem resultados de detecção completamente exatos. A geração de falsos positivos (evento normal tomado como ato de intrusão) e falsos negativos (eventos maliciosos vistos como tráfego normal) é um processo comum no uso de IDPs. Costuma-se configurar (*tune*) os IDPs de forma que a diminuir os falso negativos e aumentar os falsos positivos para que menos atos maliciosos tenham sucesso. No entanto, este comportamento sugere um overhead de processamento.

Muitos IDPs também oferecem dispositivos para compensar técnicas de evasão em ataques, que modificam o formato ou tempo da atividade maliciosa, alterando sua aparência.

A maioria dos IDPs usam múltiplas metodologias de detecção, tanto separadamente quanto integradas, para prover mais extensa e exata detecção. As principais classes de metodologias de detecção são:

- Baseado em assinatura: que compara assinaturas conhecidas com eventos observados. Novos tipos de ataques que não possuem uma assinatura não podem ser detectados;

- Detecção baseada em comportamento anômalo: compara definições e perfis de qual atividade de rede é considerada normal contra eventos observados para determinar desvios de padrão. Muito bom para novos tipos de ataques. Problemas comuns é a inclusão de atividade normal como atividade maliciosa;
- Analise de protocolo Statefull: compara perfis pré determinados de definições geralmente aceitas de atividade de protocolos com desvios nos eventos analisados. Ao contrário da metodologia anterior, esta baseia-se em perfis universais determinados e desenvolvidos por vendors que especificam como protocolos em particular devem ou não devem ser usados. Exige muito processamento e o desenvolvimento de modelos é muito difícil (quase impossível).

COMPONENTES

Os componentes típicos em uma solução IDP são:

- Sensores ou Agentes: monitoram e analisam a atividade de rede. Agentes são usados em soluções IDP *host*.
- Servidor de gerenciamento: dispositivo centralizado que recebe informações dos sensores ou agentes e as gerencia. Nesse servidor ainda são correlacionados todos os eventos de todos os sensores.
- Servidor de base de dados: é o repositório para informações de eventos gravados pelos sensores, agentes e/ou servidores de gerenciamento;
- Console: é um programa que fornece uma interface para os usuários IDP e administradores.

Adicionalmente a estes componentes, tem-se:

- Rede de gerenciamento: este um componente que pode ou não ser aplicado, conforme o projeto. É uma rede segregada apenas para os softwares de segurança, cujos dispositivos conectados são a ela por uma interface de gerenciamento.

A conexão dos dispositivos de segurança pode ser feito na própria rede de computadores, sem a necessidade de uma rede de gerenciamento. Neste caso, sugere-se a utilização de uma VLAN para prover proteção aos dispositivos e comunicações IDP. No entanto, numa VLAN, a proteção contra DDoS ou outros malware será praticamente nula.

Quando a não utilização da rede de gerenciamento, sugere-se também o uso de recursos criptográficos no tráfego de dados IDP.

ARQUITETURAS

IDP BASEADO EM REDE

Como referido anteriormente ele monitora o trafego de rede para dispositivos ou seguimentos de rede em particular e analisa a rede e a atividade de protocolos de aplicação para identificar atividade maliciosa.

Com exceção dos sensores, pode-se dizer que os IDPs baseados em rede são idênticos às outras tecnologias. Os sensores estão disponíveis em dois formatos: sensores APPLIANCE (software e hardware especiais) e sensores em SOFTWARE.

Como referido anteriormente, recomenda-se a utilização de redes de gerenciamento para a implantação da estrutura de IDPs baseados em rede. Os pontos de instalação dos sensores dentro da rede de dados da corporação é um ponto de importante observação. Os sensores pode ser instalados em dois modos:

- INLINE – quando o tráfego de rede flui pelo sensor;
- PASSIVO – quando os sensores monitoram cópias do tráfego de rede.

Geralmente recomenda-se o uso de sensores INLINE, pois assim os métodos de prevenção podem ser utilizados em prontidão, enquanto no caso dos sensores passivos os métodos de prevenção não são usados.

Os sensores podem coletar informações como o Sistema Operacional utilizados nos hosts, a versão deste sistema operacional, quais aplicações e versões são usadas para que os hosts se comuniquem com a rede, etc.

As tecnologias IDP baseadas em rede também podem controlar um registro de logs extensivo, relacionado aos dados de eventos detectados; a maioria também realiza captura de pacotes. Portanto, a maioria dos produtos desta tecnologia oferece vastos recursos de captura e detecção.

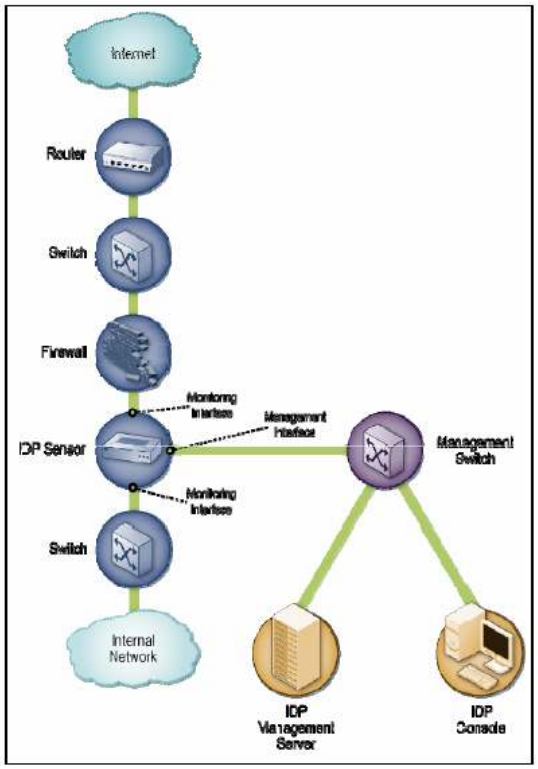
Observe-se que a combinação de metodologias como detecção baseada em assinaturas, detecção baseada em comportamento anômalo e análise de protocolo stateful, é utilizada para realizar análises detalhadas de protocolos comuns. É importante considerar esta combinação para elevar a exatidão da detecção e consequentemente da ação preventiva empregada.

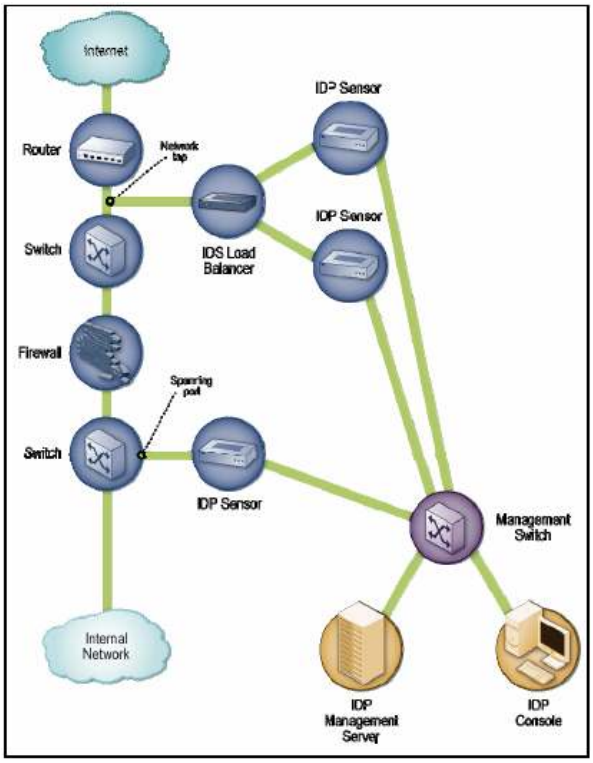
Apesar das diversas vantagens e características positivas apresentadas acima, uma grande desvantagem é a impossibilidade de detectar ataques quando o tráfego é feito de forma criptografada. Nesta situação sugere-se empregar uma solução baseada em host para efetuar a análise antes da realização da criptografia ou após os dados serem decifrados. Em outras palavras, deve-se empregar o IDP baseado em host nos pontos finais da comunicação.

Outro ponto negativo é a incapacidade dos IDPs baseados em rede não serem aptos a realizar uma análise completa quando há uma carga excessivamente grande de tráfego na rede. Recomenda-se determinar a prioridade de análise do tráfego ou simplesmente desabilitar a analise de determinados pontos quando nessa situação. Porém, os IDPs baseados em rede, por definição, acabam por ser sujeitos a ataques DDoS (grande volume de tráfego).

As características de prevenção fornecidas pelos sensores dos IDPs baseados em rede são, por exemplo, finalizar sessões TCP (reset), realização de inline Firewall, alteração de uso de largura de banda, alteração de conteúdo malicioso. Ambos, INLINE e sensores PASSIVOS, podem reconfigurar outros dispositivos de segurança, ou executar programas ou scripts de terceiros para outras ações de prevenção.

Abaixo a arquitetura recomendada para implantação tanto de sensores PASSIVOS, como sensores INLINE.





SENSOR INLINE SENSOR PASSIVO

Observe-se que os sensores INLINE atuam após o FIREWALL. Por outro lado, sensores passivos são instalados de forma a monitorar pontos chaves de redes, exatamente em sua divisão ou segregação. Alguns métodos de monitoramento usados pelos sensores passivos são: Spanning port, Network tap, IDS Load Balancer

IDP BASEADO EM REDE SEM FIO

Um IDP wireless monitora o tráfego de uma rede sem fio e analisa os protocolos de rede sem fio para identificar atividades suspeitas. Os componentes da tecnologia IDP wireless são os mesmos que a baseada em rede: sensores, consoles, servidores de dados, servidores de gerenciamento. Entretanto, um sensor de IDP wireless, monitora apenas um canal por vez, portanto, somente com amostras de tráfego – ao contrário dos sensores de IDPs baseados em rede.

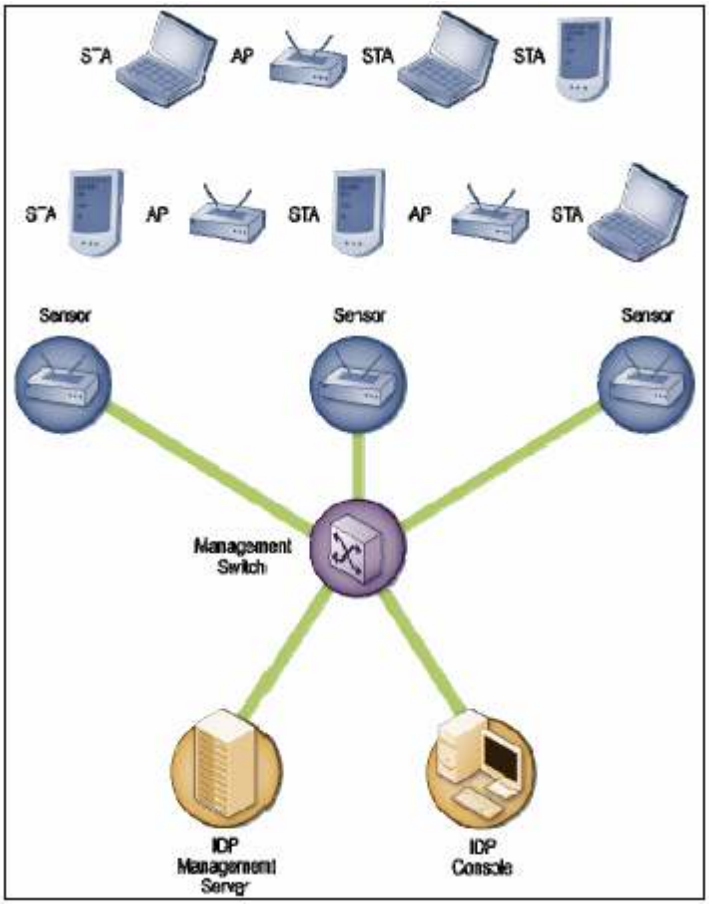
Quanto maior é o tempo de um canal monitorado, maior vai ser a probabilidade que o sensor perca atividade maliciosa nos outros canais. Para que isso não ocorra, os sensores trocam de canal diversas vezes por segundo.

Sensores IDP wireless estão disponíveis de formas diversas. Um sensor dedicado pode ser fixo ou dispositivo móvel que realiza funções IDP, mas não passa tráfego de

rede da fonte ao destino. Um outro tipo de sensor wireles disponível é o que opera em conjunto com pontos de acesso de rede sem fio (APs) ou switches sem fio Pelo fato de sensores dedicados focarem-se em detecção e não se importarem com tráfego wireless, eles oferecem recursos de detecção mais robustos. Entretanto, estes sensores são mais deficeis de se adquirir, instalar e manter do que os sensores acoplados em APs, pelo fato de exigirem outro hardware e software adicional.

Componentes de IDP wireless sempre estarão interconectados via uma rede com cabeamento. Os controles nos pontos de separação da rede sem fio e rede com cabeamento devem ser considerados, como rede de gerenciamento e etc.

A escolha da localização dos sensores para IDPs wireless é completamente diferente que em quaisquer outras tecnologias IDP. Os sensores de IDP sem fio devem ser instalados de forma que possam monitorar a abrangência do sinal sem fio. Muitas vezes os sensores devem ser instalados onde não deveria haver atividade de rede sem fio dentro da organização, analogamente têm-se os canais e bandas. Outras considerações: segurança física do sensor, abrangência, disponibilidade de conexão a rede cabeada, custo e localizações de APs/switches, conforme a figura abaixo.



IDP Wireless

Os IDPs wireless podem detectar ataques, erros de configurações e violações da política de segurança em nível de protocolo WLAN.

Os IDPs wireless, assim como as outras tecnologias IDP, necessitam de configurações a ajustes de sintonia para uma melhor performance. Porem, as tecnologias wireless normalmente oferecem uma maior exatidão na ação de detecção, muito devido ao seu escopo mais reduzido. Algumas das configurações são a definição dos APs, WLANS e STAs (estações, como laptops, PDAs. Etc) estão com acesso permitido e as características de política para cada dispositivo.

Outro ponto importante são as reestruturações físicas do ambiente organizacional que devem ser levadas em conta.

Pontos negativos de IDPs wireless são a incapacidade de detecção de ataques passivos, como o monitoramento e processamento offline do trafego wireless. Eles também são sucetíves a técnicas de evasão, especialmente àquelas que se baseiam no conhecimento do esquema de hops de canais do produto. Novamente, é importante considerar que os produtos IDP wireless só vêem parte do tráfego de um canal periodicamente. Eles também são suscetíveis a ataques de DOS.

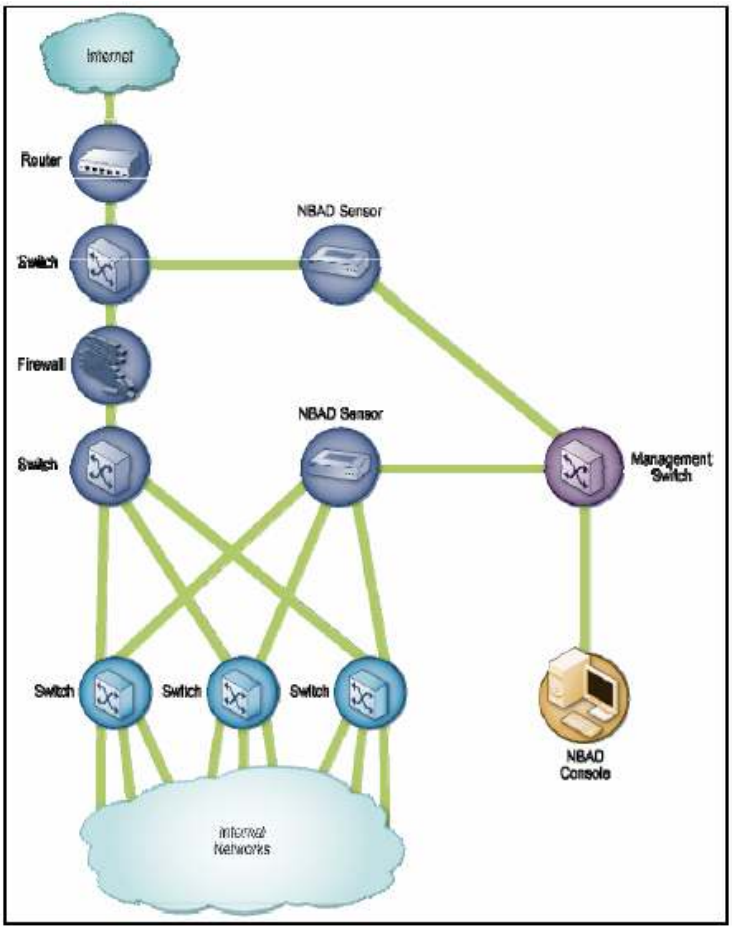
As técnicas de prevenção abordadas são a instrução para término de sessão do endpoint, e a prevenção de uma nova sessão ser estabelecida. Alguns sensores podem instruir que APs ou switches bloqueiem a atividade de um STA em particular. No entanto, este método pode bloquear a comunicação com a rede cabeada e não bloquer as atividades maliciosas do STA. Normalmente os sensores possuem dois rádios: um para monitoramento e outro para realizar ações de prevenção.

IDP BASEADO COMPORTAMENTO ANÔMALO DE REDE - NBAD

Como referido anteriormente, estes examinam e fazem análise estatística do trafego de rede para identificar ameaças que gerem um trafego de rede anormal, como ataques DDoS, escaneamento de portas e alguns tipos de malware e etc.

A maioria dos IDPs NBAD não possuem servidores de gerenciamento ou servidores de banco de dados, apenas sensores e consoles. Os sensores NBAD podem ater-se ao escaneamento direto do tráfego da rede (sniffing) ou somente nas informações de fluxo fornecidas por roteadores e outros dispositivos.

Os sensores podem ser instalados em modo passivo somente – na maioria dos IDPs NBAD – análogo aos métodos pelo IDP baseado em rede (porta de spanning, network tap). Devem ser instalados em pontos chaves da rede. – divisões ou segregações da rede, segmentos chaves de rede, como DMZ. Sensores INLINE são recomendados para uso no perímetro da rede, assim estes seriam instalados com maior proximidade dos firewalls de peímetro, sempre em frente destes, para abranger ataques que podem afetar os firewalls. A figura abaixo representa mais claramente o explicitado:



IDP NBAD

Os IDPs NBAD podem oferecer recursos extensos de obtenção de informação, coleção de informação detalhada em cada host observado e constante monitoramento da atividade de rede. Eles realizam uma compreensiva analise de log de dados relacionada aos eventos detectados. Conseguem detectar ataques dom DoS, escaneamento, worms, serviços de aplicações inesperados e violações de política. Pelo fato dos sensores trabalharem primariamente detectando desvios significativos do comportamento normal, eles são mais precisos detectando ataques que geram grande quantidade de atividade de rede em um curto período de tempo, além de ataques que tem um fluxo incomum de dados. A maioria dos produtos podem também reconstruir uma série de eventos observados para determinar a origem da ameaça.

A atualização destes produtos deve ser automática. Como resultado, configurações e determinações de "sintonia" (tuning) não são extensas. Pouquíssimos produtos NBAD oferecem customizações para assinaturas, o que é muito útil para sensores INLINE porque eles podem usar as assinaturas para encontrar e bloquer um ataque que um firewall ou roteador não tenha sido capaz de bloquear. .

É recomendável que os administradores mantenham os IDPs "cientes" da estrutura de hosts e outros dispositivos de rede (inventário), assim as configurações e

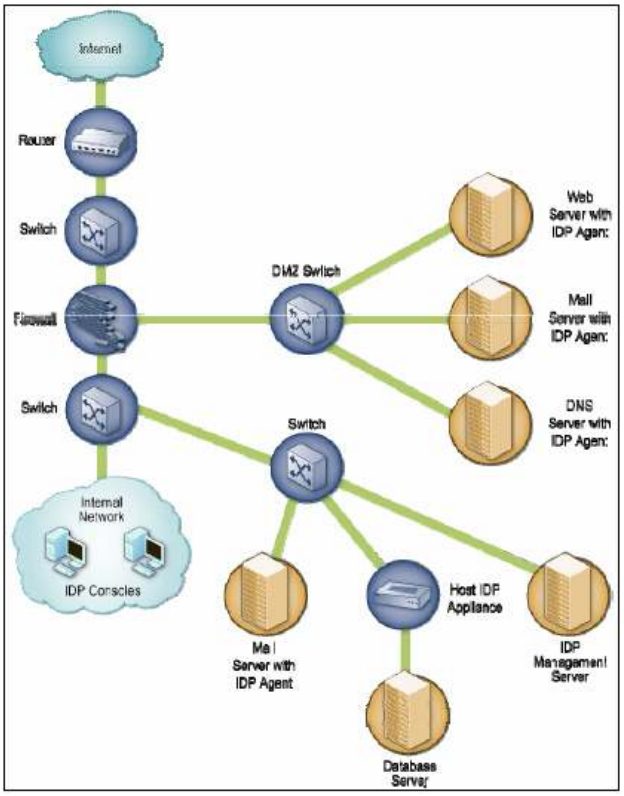
sintonia tendem a ser mais exatas com o padrão normal de tráfego de rede, gerando menos falsos positivos.

As limitações desta tecnologia são: demora de detecção, pois depende de informações advindas de dispositivos de rede como firewalls, roteadores – o que as vezes é demorado. Ataques que acontecem de forma rápida são dificilmente detectados. Uma solução para isso é a utilização pelos sensores de seu próprio recurso de captura e analise de pacotes, mas precisa de muitos recursos para realização disto.

IDP BASEADO EM HOSTS

Monitora as características de um único host e os eventos que ocorrem no mesmo de forma suspeita. Podem monitorar conexões de rede por cabeamento ou sem fio, logs de sistema, processos em execução, acessos de arquivos e modificações e alterações de configurações de sistema e aplicativos. Os AGENTES ficam instalados nos hosts de interesse, cada agente monitora a atividade em um único host, na hipótese de ter recursos, também realiza ações de prevenção. Os agentes transmitem dados aos servidores de gerenciamento. Cada agente é desenvolvido para proteger um servidor, um desktop ou laptop ou um serviço de aplicação.

A arquitetura é muito simples. Os agentes são instalados em hosts existentes nas redes das organizações e se comunicam pela rede de dados, ao invés de usar uma rede de gerenciamento. Sugere-se que o IDP Host seja instalado em servidores críticos, mas a aplicação destes em desktops, laptops e outros servidores. É importante considerar o fato de que algumas informações em hosts não podem ser monitoradas. Afigura abaixo representa o descrito:



IDP hosts

Durante a instalação de alguns agentes, é comoum a alteração da arquitetura interna dos hosts. Algumas camadas, chamadas shims ou calços, de código são implementadas. Apesar de ser menos intrusivo, a não utilização destes shims é menos precisa e as ações de prevenção menos eficientes.

Dentre os recursos estão o extensivo controle de log de dados relacionados a eventos detectados e podem ser detectados diversos tipos de atividade maliciosa. Técnicas de detecção, incluindo analise de código, analise de tráfego de rede, filtro de tráfego de rede, monitoramento de sistema de arquivos, analise de log e monitoramento de configuração de rede. A combinação de diversas técnicas de detecção tendem a ser mais precisas, pois podem monitorar diferentes características dos hosts. Devem ser determinadas quais características devem ser monitoradas para seleção dos produtos IDP.

As soluções de IDP host geralmente necessitam de bastante configurações e sintonia, devido as diferenças intrínsecas de atividade de cada host (programação, entre outros.

Limitações:

- Técnicas de detecção periódicas (poucas vezes ao dia) – incidentes podem ocorrer nesse meio tempo;
- Envio de dados de alerta aos servidores de gerenciamento em batch somente em algumas horas por dia – demora pra ações de resposta;
- Consumo de recursos no host pelos agentes;
- Conflitos com outros sistemas como firewalls pessoais, clientes VPN, etc.

Recursos de prevenção:

- Técnicas de análise de código para prevenir que códigos maliciosos sejam executados – efetivo para ataques desconhecidos;
- Analise de trafego de rede, pode impedir que trafego de entrada ou saída que contenha ataques de camada de rede, transporte ou aplicação, ataques de protocolo wireless e outras aplicações não autorizadas e protocolos.
- Filtro de trafego de rede, funciona como um firewall baseado em host e pára acessos não autorizados e aceita o uso de políticas, negando violações as mesmas.
- Monitoramento de sistema de arquivos que preveni que os arquivos sejam acessados, modificados, substituídos ou apagados, consequentemente a instalação de um malware.
- Restrições em medias removíveis;
- Detecção de ativação ou uso de dispositivos audiovisuais;
- Monitoramento do status de processos em execução e falhas de reinicialização de outros processos.

CONCLUSÃO

As tecnologias e metodologias aplicadas aos IDP variam consideravelmente, assim como variam as necessidades de uma organização para outra. Recomenda-se,também estudar e avaliar as diversas soluções IDP disponíveis no mercado para adquirir as que mais se adequam às necessidades. Múltiplas plataformas IDP de fornecedores distintos sugerem grande necessidade de interação. O uso de ferramentas como SIEM – Security Information and Event Management Software – pode auxiliar muito nessa interação.

Adicionalmente alguns requisitos gerais precisam ser definidos para grupos mais especializados de necessidades:

- Recursos de segurança, incluindo obtenção de informações, log, detecção e prevenção;
- Performance, incluindo capacidade mácima e dispositivos de performance;
- Gerenciamento, incluindo projeto e implementação, operação e manutenção e treinamento, documentação e suporte técnico;
- Custo de ciclo de vida, tanto inicial como custo de manutençao.