1.Introdução a IPSec e IDSec

Uma mudança de paradigma de arquitetura de rede se tornou necessária para se defender contra ataques rápidos e em evolução. Isso deve incluir sistemas de prevenção e detecção de baixo custo, como ***Sistemas de Detecção de Intrusão*** (***IDS***) ou sistemas de prevenção de intrusão (IPS).

Ao implementar IDS ou IPS, é importante estar familiarizado com os tipos de sistemas disponíveis, abordagens baseadas em host e em rede, o posicionamento desses sistemas e a função das categorias de assinatura.

As tecnologias IDS e IPS são implantadas como sensores. Um sensor IDS ou IPS pode estar na forma de vários dispositivos diferentes como, um roteador configurado com o software IPS, um dispositivo projetado especificamente para fornecer serviços IDS ou IPS dedicados, um módulo de rede instalado em um dispositivo de segurança adaptável (ASA), switch ou roteador.

As tecnologias IDS e IPS utilizam assinaturas para detectar padrões no tráfego da rede. Uma assinatura é um conjunto de regras que um IDS ou IPS usa para detectar atividades maliciosas. As assinaturas podem ser usadas para detectar violações graves de segurança, para detectar ataques de rede comuns e para coletar informações. Elas também podem detectar padrões de assinatura atômica ou padrões de assinatura composta.

A tabela abaixo mostra as vantagens e desvantagens de se ter um IDS/IPS.

Solução	Vantagens	Desvantagens
IDS	Nenhum impacto na rede Nenhum impacto na rede se houver falha do sensor Sem impacto na rede se houver sobrecarga do sensor	Ação de resposta não pode parar pacotes de gatilho Ajuste correto necessário para ações de resposta Mais vulnerável a técnicas de evasão de segurança de rede
IPS	Interrompe pacotes de gatilho Pode usar técnicas de normalização de fluxo	Problemas de sensor podem afetar o tráfego da rede A sobrecarga do sensor afeta a rede Algum impacto na rede

1.1 IPS de host (HIPS)

O IPS baseado em host é um software instalado em um host para monitorar e analisar atividades suspeitas. **Uma vantagem significativa do HIPS** é de que ele pode monitorar e proteger o sistema operacional e os processos críticos do sistema que são específicos para esse host. Com conhecimento detalhado do sistema operacional, o HIPS pode monitorar

atividades anormais e impedir que o host execute comandos que não correspondem ao comportamento típico.

Esse comportamento suspeito ou mal-intencionado pode incluir atualizações de registro não autorizadas, alterações no diretório do sistema, execução de programas de instalação e atividades que causam estouros de buffer. O tráfego de rede também pode ser monitorado para impedir que o host participe de um ataque de negação de serviço (DoS) ou faça parte de uma sessão de FTP ilícita.

HIPS também podem ser pensados como uma combinação de software antivírus, antimalware e um firewall. **Porém, uma desvantagem do HIPS** é que ele opera apenas a nível local. Ele não tem uma visão completa da rede ou eventos coordenados que possam estar acontecendo em toda a rede. Para ser eficaz em uma rede, o HIPS deve ser instalado em cada host e ter suporte para cada sistema operacional.

A tabela abaixo mostra mais das vantagens e desvantagens do HIPS

Vantagens	Desvantagens
Fornece proteção específica para um sistema operacional host; Fornece proteção em nível de aplicação e sistema operacional; Protege o host depois que a mensagem é descriptografada	Dependente do sistema operacional; Deve ser instalado em todos os hosts

1.2 IPS baseado em rede (NIPS)

Pode ser implementado usando um dispositivo IPS dedicado ou não dedicado. As implementações de IPS baseadas em rede são um componente crítico da prevenção de intrusões. As soluções IDS/IPS baseadas em host são integradas a uma implementação IPS baseada em rede para garantir uma arquitetura de segurança robusta

Os sensores detectam atividades maliciosas e não autorizadas em tempo real e podem agir quando necessário.

Os sensores IPS baseados em rede podem ser implementados de várias maneiras como, dispositivos Cisco Firepower, dispositivo de firewall ASA e roteador ISR. O hardware de todos os sensores baseados em rede inclui três componentes.

- **NIC:** O IPS baseado em rede deve poder conectar-se a toda rede, tal como Ethernet, Fast Ethernet e Gigabit Ethernet.
- **Processador:** A prevenção de intrusões requer poder de processamento para realizar análise de detecção de intrusão e correspondência de padrões
- **Memória:** A análise de detecção de intrusão é intensiva em memória. Essa memória afeta diretamente a capacidade de um IPS baseado em rede para detectar um ataque com eficiência e precisão.

Os sensores IDS/IPS **podem operar em modo in-line ou modo promíscuo**.

Os pacotes não fluem através do sensor no modo promíscuo. O sensor analisa uma cópia do tráfego monitorado, não do pacote real enviado. **A vantagem de operar no modo promíscuo** é que o sensor não afeta o fluxo do pacote com o tráfego encaminhado. A desvantagem de operar neste modo é que o sensor não pode impedir que o tráfego malicioso atinja seu alvo pretendido para certos tipos de ataques, como ataques atômicos.

As ações de resposta implementadas por dispositivos promíscuos são respostas pós-evento e muitas vezes exigem assistência de outros dispositivos de rede para responder a um ataque. Tais ações de resposta podem impedir algumas classes de ataques. Contudo, em ataques atômicos, o único pacote tem a possibilidade de alcançar o sistema de destino antes que o sensor promíscuo possa aplicar uma modificação ACL de um dispositivo controlado.

Operar em modo in-line coloca o IPS diretamente no fluxo de tráfego e torna as taxas de encaminhamento de pacotes mais lentas adicionando latência. Este modo permite que o sensor para ataques, derrubando o tráfego malicioso antes de atingir o alvo pretendido, proporcionando assim um serviço de proteção. Além de processar informações nas camadas 3 e 4, ele analisa o conteúdo e a carga útil dos pacotes para ataques incorporados mais sofisticados (3 até 7). Essa análise mais profunda permite que o IPS identifique, pare e bloqueie os ataques que passariam por um dispositivo de firewall tradicional.

Um sensor IPS contém dois componentes:

- **Detecção IPS e mecanismo de aplicação:** Para validar o tráfego, o mecanismo de detecção compara o tráfego de entrada com assinaturas de ataque conhecidas que são incluídas no pacote de assinatura de ataque IPS.
- **Pacote de assinatura de ataque IPS:** Esta é uma lista de assinaturas de ataques conhecidos que estão contidas em um arquivo. O pacote de assinatura é atualizado com frequência à medida que novos ataques são descobertos.

Existem dois tipos de assinaturas baseadas em termos:

- **Conjunto de regras comunitárias:** Este conjunto oferece cobertura limitada contra ameaças, com foco em resposta reativa às ameaças de segurança versus trabalho proativo de pesquisa. Há 30 dias de acesso atrasado, as assinaturas atualizadas no conjunto de regras da comunidade, e esta assinatura não dá direito ao cliente ao suporte Cisco.
- **Conjunto de regras de assinantes:** Este conjunto oferece a melhor proteção contra ameaças. Ele inclui coberturas antes das explorações usando o trabalho de pesquisa dos especialistas em segurança Cisco Talos. O conjunto de regras de assinante também fornece o acesso mais rápido às assinaturas atualizadas em resposta a um incidente de segurança ou à descoberta proativa de uma nova ameaça. Esta assinatura é totalmente suportada pela Cisco.

Uma rede deve ser capaz de identificar o tráfego malicioso de entrada para pará-lo. Conceitualmente semelhante ao arquivo virus.dat usado por antivírus, uma assinatura é um conjunto de regras que um IDS e um PS usam para detectar atividades típicas de intrusão. As assinaturas identificam exclusivamente vírus, worms, anomalias de protocolo e tráfego malicioso específico.

Um fluxo de pacotes malicioso tem um tipo específico de atividade e assinatura. Os sensores IPS devem ser ajustados para procurar assinaturas correspondentes ou padrões de tráfego anormais. À medida que os sensores verificam pacotes de rede, eles usam assinaturas para detectar ataques conhecidos e responder com ações predefinidas. Um sensor IDS ou IPS examina o fluxo de dados usando muitas assinaturas diferentes. As assinaturas também têm três atributos distintos dos quais são os tipos, o gatilho e a ação.

Algumas ameaças podem ser identificadas em um pacote, enquanto outras ameaças podem exigir muitos pacotes e suas informações de estado para identificar uma ameaça. Existem dois tipos de assinaturas:

- **Assinaturas atômicas:** Este é o tipo mais simples de assinatura porque um único pacote, atividade ou evento identifica um ataque. O IPS não precisa manter informações de estado e análise de tráfego, geralmente pode ser realizado de forma muito rápida e eficiente.
- **Assinaturas compostos:** Também chamado de assinatura stateful porque o IPS requer várias partes de dados para corresponder a uma assinatura de ataque. O IPS também deve manter informações estatais, que é referido como o horizonte de eventos.O comprimento de um horizonte de eventos varia de uma assinatura para outra.

O alarme da assinatura para um sensor IPS pode ser qualquer coisa que possa sinalizar confiantemente uma violação da intrusão ou da política de segurança. Um IPS baseado em rede pode desencadear uma ação de assinatura se detectar um pacote com uma carga útil que contenha uma string específica que esteja indo a uma porta TCP específica.

Ele é análogo ao alarme em um sistema de segurança doméstica. O mecanismo de disparo para um alarme de assinatura pode ser um detector de movimento. Quando o alarme do assinante está ativado, o movimento de um indivíduo que entra em uma sala é detectado. Isso aciona o alarme.

Esses mecanismos desencadeadores podem ser aplicados a assinaturas atômicas e compostas. Os mecanismos de desencadeamento podem ser simples ou complexos. Cada IPS incorpora assinaturas que usam um ou mais desses mecanismos de disparo básicos para acionar ações de assinatura.

Há quatro categorias gerais do disparador da assinatura IPS, mostrados na tabela abaixo.

Tipo de detecção	Vantagens

Detecção baseada em padrões	Conhecido como detecção baseado em assinatura Mecanismo de disparo mais simples, uma vez que procura um padrão atômico ou composto específico e pré-definido Um sensor IPS compara o tráfego de rede a um banco de dados de ataque conhecidos e adiciona um alarme ou impede a comunicação se uma correspondência for encontrada
Detecção baseada em anomalias	Também conhecido como detecção baseada em perfil Envolve primeiro definir um perfil do que é considerado atividade normal de rede ou host Esse perfil normal geralmente é definido monitorando o tráfego e estabelecendo uma linha de base Uma vez definida, qualquer atividade além de um limite especificado no perfil normal gerará gatilho e uma ação de assinatura
Detecção baseada em políticas	Também conhecido como detecção baseada em comportamento Embora semelhante à detecção baseada em padrões, um administrador define manualmente comportamentos suspeitos com base na análise histórica O uso de comportamentos permite que uma única assinatura abranja toda uma classe de atividades sem precisar especificar cada situação individual
Detecção honeypot	A detecção baseada em honeypot usa um servidor como um servidor de chamariz para atrair ataques O objetivo de um servidor chamariz é atrair ataques para longe de dispositivos de produção Permite que os administradores analisem ataques recebidos e padrões de tráfego mal-intencionados para ajustar suas assinaturas de sensores

Quando uma assinatura detecta a atividade para a qual está configurada, a assinatura aciona uma ou mais ações. Dependendo do sensor IPS, várias ações podem ser ativadas. A tabela abaixo lista algumas destas ações.

Categoria de alerta	**Ação específica**	**Descrição**
Gerar um alerta	Produzir alerta	O IPS envia eventos como alertas
	Produzir alerta detalhado	O IPS envia um alerta de evento detalhado
Registrar a atividade	Pacotes de invasores de log	Registra o pacote do endereço IP do invasor e envia um alerta
	Pacotes de par de	Registra pacotes do endereços IP da

	log	vítima e do invasor e envia um alerta
	Log pacotes de vítimas	Registra pacotes do endereço IP da vítima e envia um alerta
Negar a atividade	Negar pacote em linha	Termina o pacote
	Negar conexão em linha	Termina o pacote atual e os pacotes futuros neste fluxo TCP
	Negar atacante em linha	Termina o pacote atual e os pacotes futuros deste endereço do invasor por um período de tempo especificado
Redefina a conexão TCP	Redefinir conexão TCP	Envia restaurações TCP para sequestrar e terminar o fluxo TCP
Bloquear atividades futuras	Solicitar conexão de bloco	Envia uma solicitação a um dispositivo de bloqueio para bloquear essa conexão
	Solicitar host de bloco	Envia uma solicitação para um dispositivo de bloqueio para bloquear esse host invasor
	Solicitar trap SNMP	Envia uma solicitação ao componente do aplicativo de notificação do sensor para executar a notificação SNMP

Os mecanismos de disparo **podem gerar alarmes que são falsos positivos ou falsos negativos**. Esses alarmes devem ser abordados ao implementar um sensor IPS. Verdadeiros positivos e verdadeiros negativos são desejáveis e indicam que o IPS está funcionando corretamente. Falsos positivos e falsos negativos são indesejáveis e devem ser investigados.

Tipo de alarme	Atividade da rede	Atividade IPS	Resultado
Verdadeiro positivo	O tráfego de ataque	Alarme gerado	Ajuste ideal
Verdadeiro negativo	Tráfego normal de usuários	Nenhum alarme gerado	Ajuste ideal
Falso positivo	Tráfego normal de usuários	Alarme gerado	Sintonizar alarme
Falso negativo	O tráfego de ataque	Nenhum alarme gerado	Sintonizar alarme

2.Verdadeiro positivo (desejável)

Isto é usado quando o IPS gera um alarme porque detectou o tráfego conhecido do ataque. O alerta foi verificado como um incidente de segurança real e também indica que a regra IPS funcionou corretamente.

2.1 Verdadeiro negativo (desejável)
Isso é usado quando o sistema está funcionando como esperado. Nenhuma letra é emitida porque o tráfego que está passando pelo sistema está livre de ameaças.

2.2 Falso positivo (indesejável)
Isso é usado quando um IPS gera um alarme depois de processar o tráfego normal do usuário que não deveria ter acionado um alarme. O IPS deve ser ajustado para alterar esses tipos de alarme para verdadeiros negativos. O alerta não indica um incidente de segurança real. A atividade benigna que resulta em um falso positivo é às vezes referida como um gatilho benigno. Os falsos positivos são caros porque devem ser investigados.

2.3 Falso negativo (perigoso)
Isso é usado quando um IPS não consegue gerar um alarme e ataques conhecidos não estão sendo detectados. Isso significa que os exploits não estão sendo detectados pelos sistemas de segurança existentes. Esses incidentes podem passar despercebidos por um longo período de tempo, e a perda e danos contínuos de dados podem resultar. O objetivo é que esses tipos de alarmes gerem alarmes positivos verdadeiros.

As organizações agora têm três opções disponíveis para fornecer serviços de prevenção de intrusões.

- **IPS da próxima geração de Cisco Firepower (NGIPS):** Estes são dispositivos dedicados à prevenção de ameaças em linha que fornecem eficácia líder do setor contra ameaças conhecidas e desconhecidas.
- **Cisco Snort IPS:** Este é um serviço IPS que possa ser permitido em um ISR da segunda geração. Note que o Cisco 4000 ISRs já não apoia o Cisco IOS IPS.
- **Servidor IPS do Snort Externo:** Isto é similar à solução IPS do Snort de Cisco, mas exige uma porta promíscua e um Snort externo IDS/IPS.
- **NGIPS:** NGIPS são dispositivos IPS dedicados e são construídos sobre a tecnologia aberta do núcleo do Snort e usam regras IPS, vulnerabilidade focada e inteligência de segurança baseada em IP, URL- e DNS encaixada, fornecida pela Cisco Talos.

Os recursos do NGIPS incluem o seguinte:

- Regras IPS que identificam e bloqueiam o tráfego de ataque direcionado às vulnerabilidades da rede
- Defesa totalmente integrada contra malware avançado, incorporando análise avançada de rede e atividade de endpoint
- Tecnologia de sandbox que usa centenas de indicadores comportamentais para identificar ataques de dia zero e ataques de evasão
- Inclui visibilidade e controle de aplicativos (AVC), Cisco Advanced Malware Protection (AMP) para redes e filtragem de URL.

3.Sistemas de detecção de intrusão

Conhecido como ***Intrusion Detection System*** (***IDS***), é uma tecnologia de segurança cibernética que tem como objetivo monitorar e analisar o tráfego de rede e a atividade dos sistemas em busca de comportamentos anômalos e potenciais ameaças.

O funcionamento do IDS pode ser dividido em algumas etapas principais:

- **Coleta de dados:** O IDS coleta dados de diversas fontes, como logs de eventos, registros de atividades de rede, registros de sistemas e outros dados relevantes. Essa coleta de informações é contínua e abrange todo o ambiente de rede e sistemas que está sendo monitorado.
- **Análise do tráfego e comportamento:** Após a coleta dos dados, o IDS analisa o tráfego de rede e o comportamento dos sistemas em busca de padrões suspeitos ou atividades incomuns. Essa análise é feita com base em regras pré-definidas, algoritmos de aprendizado de máquina ou técnicas estatísticas.
- **Comparação com assinaturas de ataques conhecidos:** O IDS também compara o tráfego e o comportamento observado com uma base de dados de assinaturas de ataques conhecidos. Essas assinaturas são padrões de atividade que foram previamente identificados como indicadores de ataques específicos, como malware, worms ou tentativas de intrusão.
- **Geração de alertas:** Quando o IDS detecta atividades que correspondem a padrões de comportamento suspeitos ou assinaturas de ataques conhecidos, ele gera alertas para notificar os administradores de segurança. Esses alertas podem ser exibidos em um painel de controle, enviados por e-mail ou outros meios de comunicação.
- **Respostas e ações:** Com base nos alertas recebidos, os administradores de segurança podem tomar ações adequadas para investigar e responder às potenciais ameaças. Isso pode incluir isolar sistemas comprometidos, bloquear endereços IP suspeitos, realizar análises mais aprofundadas ou tomar outras medidas para conter e mitigar os riscos.

3.1 Network-based Intrusion Detection Systems (NIDS)

- **Posicionamento:** Os NIDS são implantados em pontos estratégicos da rede, geralmente em locais onde o tráfego converge, como roteadores, switches ou firewalls. Eles monitoram o tráfego que passa por esses pontos, analisando pacotes de dados em busca de padrões suspeitos ou atividades maliciosas.
- **Análise de tráfego:** Os NIDS inspecionam pacotes de dados à medida que eles atravessam a rede, aplicando regras, assinaturas e algoritmos de análise comportamental para identificar atividades suspeitas. Isso pode incluir identificar tentativas de intrusão, varreduras de portas, tráfego incomum ou comportamento anômalo.
- **Alertas e notificações:** Quando o NIDS detecta algo fora do padrão ou uma possível intrusão, ele gera alertas para os administradores de segurança. Esses alertas podem ser visualizados em um console de gerenciamento ou enviados por e-mail, permitindo uma resposta rápida e adequada.

3.2 Host-based Intrusion Detection Systems (HIDS)

- **Implantação em hosts:** Os HIDS são instalados em cada host individual dentro da rede, como computadores, servidores ou dispositivos finais. Eles operam em nível de sistema operacional e monitoram atividades locais em um host específico.
- **Monitoramento de eventos locais:** Os HIDS monitoram eventos e atividades no host, como alterações de arquivos, atividades de login, tentativas de execução de comandos privilegiados e outras ações relevantes. Eles comparam essas atividades com regras e assinaturas de ataques conhecidos.
- **Diferentes níveis de detecção:** Os HIDS podem detectar atividades que podem não ser visíveis no tráfego de rede, como ações realizadas diretamente no host ou comportamento malicioso que não deixa rastros na rede.
- **Respostas no próprio host:** Quando um HIDS detecta uma atividade suspeita ou intrusão, ele pode tomar medidas diretamente no host afetado, como bloquear o tráfego, desligar processos maliciosos ou enviar alertas locais.

4.Cisco IPS

O Cisco IOS IPS detecta atividades suspeitas, ele responde antes que a segurança de rede possa ser comprometida, registra o evento como mensagem do syslog do Cisco IOS ou através do SDEE. O administrador de rede poderia configurar o Cisco IOS IPS para escolher a resposta apropriada a várias ameaças.

Um exemplo de configuração seria que, se envia um alarme a um servidor de syslog ou a uma interface de gerenciamento centralizada, descarta o pacote, reseta a conexão, nega o tráfego do endereço IP de origem da ameaça por um período de tempo especificado, nega o tráfego na conexão para a qual a assinatura foi vista por uma quantidade específica de tempo.

Snort é uma rede aberta IPS que realiza análise de tráfego em tempo real e gera alertas quando as ameaças são detectadas em redes IP. Ele também pode realizar análise de protocolo, pesquisa ou correspondência de conteúdo e detectar uma variedade de ataques e sondagens.

Snort é a solução IPS mais amplamente utilizada no mundo. É um IPS de rede de código aberto que executa análise de tráfego em tempo real e gera alertas quando ameaças são detectadas em redes IP. Ele também pode realizar análise de protocolo, pesquisa de conteúdo ou correspondência e detectar uma variedade de ataques e sondas, como estouros de buffer, varreduras de portas furtivas e assim por diante.

Snort IPS pode ser executado com outros recursos de segurança integrados nos 4000 Series ISRs, tais como VPN, firewalls baseados em zona do Cisco IOS e Cisco Cloud Web Security. Isso permite que o ISR forneça proteção abrangente contra ameaças em um espaço pequeno. Snort IPS integrado em um ISR é uma alternativa eficaz na redução de custos para locais de filial porque um dispositivo de firewall separado não é exigido.

Snort IPS no 4000 Series ISR fornece as seguintes funcionalidades:

- **IDS e modo IPS:** Configurar o modo de detecção ou prevenção de ameaças. No modo de prevenção, o tráfego de ataque será deixado cair
- **Três níveis de assinatura:** Snort fornece três níveis de proteção de assinatura. A conectividade, equilibrada e segurança. O nível de segurança é o mais seguro, pois permite que o maior número de assinaturas seja verificado.
- **Uma lista permitida:** Isto fornece a capacidade de desligar determinadas assinaturas e ajuda a evitar falsos positivos tais como o tráfego legítimo que desencadeia uma ação IPS. Até 1000 entradas podem ser apoiadas na lista permitida.
- **Snort monitoramento de saúde:** O Cisco IOS Software mantém o controle da integridade do motor do Snort que está sendo executado no recipiente do serviço.
- **Falha em abrir e fechar:** No caso da falha do motor IPS, o roteador pode ser configurado para obstruir o fluxo de tráfego ou contornar a verificação IPS até que o motor do Snort recupere
- **Atualização de assinatura:** Atualizações automáticas e manuais são suportadas. Snort IPS pode transferir o pacote da assinatura diretamente do cisco.com ou de um lugar de recurso local sobre HTTP e HTTPS
- **Registro de eventos:** Os logs IPS podem ser enviados a um coletor de log independente ou incluídos junto com o córrego do syslog do roteador. Enviar logs IPS ajuda separadamente se a ferramenta de gerenciamento de eventos de segurança é diferente do servidor de syslog regular.

O motor do Snort é executado em um recepiente do serviço virtual em Cisco ISRs Series 4000. **Um contêiner de serviço virtual** é uma máquina virtual que é executada no sistema operacional do roteador ISR. Os containers de serviço são aplicativos que podem ser hospedados diretamente em plataformas de roteamento do Cisco IOS XE. Esses aplicativos usam os aspectos Linux do sistema operacional IOS XE para hospedar tanto Linux Virtual Containers (LXC) quanto Kernel Virtual Machines (KVM). O contêiner do Snort é distribuído como um arquivo aberto do dispositivo da virtualização (OVA) que é instalado no roteador.

Ao contrário do IOS IPS, o Snort IPS pode usar o poder do computador do contêiner de serviço para escalar a segurança com a plataforma sem afetar as capacidades de roteamento ou a outra funcionalidade do plano de dados. O serviço virtual suporta três perfis de recursos que indicam como o contêiner Snort usa recursos de CPU, RAM e Flash ou disco do sistema.

As assinaturas do Snort IPS são entregues automaticamente ao usar ISR pelo Cisco Talos. Há atualmente mais de 30.000 assinaturas no conjunto de regras do Snort. Ele também suporta a capacidade de personalizar conjuntos de regras e fornece recursos centralizados de implantação e gerenciamento para ISRs série 4000.

Snort pode ser ativado em um dos seguintes modos:

- **Modo IPS:** Além da detecção de intrusão, são tomadas ações para evitar ataques

- **Modo IDS:** Snort inspeciona o tráfego e relata alertas, mas não toma nenhuma ação para impedir ataques

No modo de detecção e da prevenção da intrusão da rede, o Snort executa as seguintes ações, monitoramento do tráfego de rede analisando em relação a um conjunto de regras definidos, execução da classificação de ataque, invocação de ações contra regras correspondentes.

O Snort IPS monitora o tráfego e relata eventos a um servidor de log externo ou ao SYSLOG IOS. Permitir o registro ao SYSLOG IOS pode afetar o desempenho devido ao volume potencial de mensagens de log. As ferramentas externas de monitoração de terceiros que apoiam logs do Snort podem ser usadas para a coleta e a análise do registro.

A tabela abaixo lista recursos e benefícios do Snort IPS

Recurso	Benefícios
IDS baseado em assinatura e IPS	Snort IPS de código aberto, capaz de executar análise de tráfego em tempo real e registro de pacotes em redes IP, é executado no recipiente de serviço ISR Series 4000 se a necessidade de distribuir um dispositivo adicional no ramo
Atualizações do conjunto de regras Snort	As atualizações do conjunto de regras do Snort para ISRs series 4000 são geradas pelo Cisco Talos, um grupo de especialistas de segurança de rede de ponta que trabalham 24 horas por dia para descobrir, avaliar e responder proativamente às últimas tendências em atividades de pirataria, tentativas de intrusão, malware e vulnerabilidades
Regra Snort de puxar	O roteador poderá transferir grupos de regra diretamente do cisco.com ou do snort.org a um servidor local, usando comandos únicos ou atualizações automatizadas periódicas
Snort regra definida	Uma ferramenta de gerenciamento centralizado pode empurrar os conjuntos de regras baseados na política pré-configurada, em vez do roteador que transfere diretamente por conta própria
Listagem de assinatura permitida	A listagem permitida permite a desativação de determinadas assinaturas do conjunto de regras. As assinaturas desativadas podem ser reativadas a qualquer momento

Snort IPS para o 4000 Series ISRs consiste em dois componentes:

- **Motor Snort:** Este é o mecanismo de detecção e aplicação IPS que está incluído na licença Security (SEC) para ISRs 4000 Series
- **Assinaturas do software de regras do Snort para atualizações de assinatura:** Os conjuntos de regras do Snort para se manter em dia com a proteção contra ameaças mais recentes são assinaturas baseadas em prazo, disponíveis por um ou três anos.

Para abordar o cenário de ameaças em rápida evolução, é importante garantir que as assinaturas estejam tão atualizadas quanto possível. Existem dois tipos de assinaturas baseadas em termos:

- **Conjunto de regras da comunidade:** Disponível gratuitamente, esta assinatura oferece cobertura limitada contra ameaças. O conjunto de regras da comunidade concentra-se na resposta reativa às ameaças à segurança versus trabalho de pesquisa proativo. Há também um acesso atrasado de 30 dias a assinaturas atualizadas.
- **Conjunto de regras de assinante:** Disponível por uma taxa, este serviço oferece a melhor proteção contra ameaças. Inclui cobertura de exploits avançados usando o trabalho de pesquisa dos especialistas em segurança Cisco Talos. O conjunto de regras de assinante também fornece acesso mais rápido às assinaturas atualizadas em resposta a um incidente de segurança ou à descoberta proativa de uma nova ameaça. Esta assinatura é totalmente suportada pela Cisco.

Os aplicativos tais como o Snort IPS podem ser transferidos arquivos pela rede e hospedados em roteadores. Os containers de serviço são suportados na maioria das plataformas IOS XE. IOS XE é baseado na arquitetura Linux e suporta hospedagem de máquina virtual.

O motor Snort é executado como um aplicativo do recipiente do serviço Linux no ISR 4000. Isso fornece recursos de computação dedicados que são executados independentemente da carga da CPU do plano de dados. Ele também torna mais fácil para o motor Snort ser atualizado regularmente.

Especificamente, o motor Snort no 4000 Series ISR é executado como um aplicativo de contêiner. O 4000 Series ISR usa uma CPU multi-core, e o Cisco IOS-XE tem a capacidade de alocar esses núcleos para funções de plano de controle ou de plano de dados. Os recursos de computação não utilizados pelas funções do plano de controle podem ser usados para executar outros serviços. Uma infraestrutura de contêiner Linux hospeda esses aplicativos. Os aplicativos executados nesta infraestrutura de contêiner podem ter uma integração mais apertada com o Cisco IOS Software.

No Snort IPS, as assinaturas são configuradas usando "*rules*". Estas regras servem como os alarmes da assinatura comparando o tráfego que entra com às regras do Snort. O tráfego corresponde a um cabeçalho de regra e gera uma ação. O cabeçalho de regra é conceitualmente similar a uma instrução ACL.

Snort pode ser permitido no modo IDS ou no modo IPS. Snort IDS pode executar as seguintes três ações: Alert (gera um alerta usando o método de alerta selecionado); Log (registra o pacote); Pass (ignora o pacote).

O modo IPS do Snort pode executar todas as ações do IDS mais o seguinte.

- **Drop:** Bloqueia e registra o pacote

- **Reject:** Bloqueia o pacote, registra-o e envia então uma redefinição de TCP se o protocolo for TCP, ou uma mensagem inalcançável da porta ICMP se o protocolo for UDP
- **Sdrop:** Bloqueia o pacote, mas não o registra

Um cabeçalho da regra do Snort igualmente contém opções da regra para fornecer a informação adicional para a regra. As opções são separadas por ponto-e-vírgula e as palavras-chave de opção de regra são separadas de seus argumentos usando dois pontos. A tabela abaixo descreve a regra geral comum e as opções de regra de detecção no cabeçalho da regra de mostra.

Opção de regra	Ação específica
msg:	Esta é uma string de texto simples que fornece uma mensagem significativa para a saída quando a regra corresponde
flow:	Especifica a direção do tráfego de rede
content: distante: / offset:	Uma opção de regra de detecção que permite que o criador de regras defina regras que buscam conteúdo específico na carga útil do pacote e adicionam a resposta com base nesses dados. Estes dados de opção podem conter texto misto e dados binários
within: / depth:	Palavras-chave de regras de detecção que permitem que o criador de regras especifique onde começar a pesquisar em relação ao início da carga útil ou ao início de uma correspondência de conteúdo
pcre	Uma palavra-chave de regra de detecção que permite que as regras sejam escritas usando "expressões regulares compatíveis com perl" que permite correspondências mais complexas
byte_test	Uma palavra-chave de regra de detecção que permite que uma regra teste um número de bytes contra um valor específico em binário
metadata:	Permite que um criador de regras incorpore informações adicionais sobre a regra
reference:	Permite que as regras incluam referências a fontes externas de informação
classtype:	Identifica o efeito potencial do que seria um ataque bem-sucedido
sid / rev	O ID da assinatura (sid) é um identificador único para cada regra, tornando-as fáceis de identificar. Deve ser usado como o rev (revisão) palavra-chave para indicar a versão atual da regra

Os pacotes que chegam em relações permitidas do Snort são inspecionados como segue:

- O Cisco IOS Software passa para a frente os pacotes a serem inspecionados ao motor IPS do Snort usando uma interface interna do grupo de porta virtual (VPG)
- Snort IPS inspeciona o tráfego e torna a ação necessária
- Snort deixa cair os pacotes associados com fluxos ruins. Os bons pacotes de fluxo são retornados de volta ao roteador para processamento adicional

A troca de pacotes entre os aplicativos de contêiner e os planos de dados IOS é feita usando interfaces VPG. Essas interfaces roteadas são conectadas através do plano traseiro do roteador. A interface correspondente no lado do contêiner aparecerá como porta Ethernet virtual.

Snort IPS requer duas interfaces VPG.

- **Interface de gerenciamento:** Esta é a relação que é usada aos logs da fonte ao coletor do log e recuperando atualizações da assinatura do cisco.com. Por esta razão, esta relação exige um endereço IP roteável
- **Interface de dados:** Esta é a relação que é usada para enviar o tráfego de usuário entre o serviço do recipiente virtual do Snort e o plano de encaminhamento de roteador.

5.Ferramentas de detecção/prevenção de intrusões

5.1 Switched Port Analyzer (SPAN) ou Mirror Port

É uma funcionalidade presente em dispositivos de rede, como switches e roteadores, que permite a monitoração do tráfego de rede em tempo real sem interromper o fluxo normal de dados. O **SPAN permite que os administradores de rede capturem o tráfego de determinadas portas ou VLANs e redirecionem esse tráfego para uma porta específica, chamada porta de monitoramento ou porta espelho**.

Essa porta é usada para conectar um dispositivo de análise, como um IDS/IPS ou um analisador de pacotes, que irá analisar e inspecionar o tráfego para fins de segurança, monitoramento ou solução de problemas. Veja como funciona:

- **Configuração do SPAN:** Para configurar o SPAN, um administrador de rede acessa o switch ou roteador e define a porta de origem (a porta ou VLAN de onde o tráfego será copiado), a porta de destino ou porta de monitoramento (onde o tráfego copiado será enviado) e a direção do tráfego a ser espelhado (entrada, saída ou ambos).
- **Cópia de tráfego:** Uma vez configurado, o switch começa a copiar o tráfego da porta de origem ou VLAN especificada para a porta de monitoramento, em tempo real. A cópia inclui tanto o tráfego de entrada como o de saída, dependendo da configuração feita pelo administrador.
- **Inspeção de tráfego:** O tráfego copiado na porta de monitoramento é enviado ao dispositivo de análise (por exemplo, um IDS/IPS) conectado a essa porta. O dispositivo de análise examina e inspeciona os pacotes, procurando por atividades suspeitas,

ameaças, anomalias ou outras informações úteis para fins de monitoramento ou segurança.

- **Análise de pacotes:** O dispositivo de análise pode executar várias ações, como identificação de ameaças, criação de relatórios, geração de alertas, registro de eventos e outras análises específicas, dependendo de suas funcionalidades e configurações.
- **Benefícios do SPAN:** O SPAN (Mirror Port) oferece a capacidade de monitorar o tráfego de rede em tempo real sem impactar o fluxo normal de dados. Isso é especialmente útil para fins de segurança, permitindo a inspeção de tráfego em busca de atividades maliciosas ou comportamentos anômalos, sem interromper as operações da rede.

5.2 Network Test Access Point (TAP)

É um dispositivo de rede usado para monitorar o tráfego de dados em tempo real sem interromper o fluxo normal de dados, proporcionando uma visibilidade completa e precisa do tráfego de rede. Existem dois tipos principais de TAP: ***Passive TAP*** (***TAP passivo***) e ***Active TAP*** (***TAP ativo***).

O TAP é amplamente utilizado em ambientes de monitoramento de rede, como para a implantação de dispositivos de segurança, como IDS/IPS, analisadores de pacotes e soluções de monitoramento de desempenho de rede. É uma ferramenta valiosa para solucionar problemas de rede, permitindo que os administradores de rede tenham uma visibilidade completa do tráfego em tempo real e identifiquem possíveis problemas.

5.2.1 TAP passivo

- **Design e funcionamento:** O Passive TAP é um dispositivo que opera de forma passiva e não requer fonte de energia própria. Ele é geralmente colocado entre dois dispositivos de rede, como switches, roteadores ou servidores, atuando como um divisor de luz. O TAP possui portas de entrada e saída, onde os cabos de rede conectados ao dispositivo de origem são duplicados para que o tráfego completo, tanto em direção de entrada quanto de saída, seja copiado para a saída do TAP.
- **Divisão de sinal:** O TAP passivo usa tecnologia de divisão de sinal óptico ou elétrico para fazer uma cópia exata dos pacotes de dados que passam pelo dispositivo de origem, sem causar qualquer interrupção no fluxo de tráfego normal.
- **Conectividade não-invasiva:** Como o Passive TAP não requer energia e opera apenas como um ponto de conexão passiva, não há risco de falhas de energia ou de afetar a operação normal da rede.

5.2.2 TAP ativo

- **Design e funcionamento:** O Active TAP é um dispositivo que requer uma fonte de energia própria para funcionar. Ele também possui portas de entrada e saída, mas ao contrário do TAP passivo, ele não apenas copia o tráfego de rede, mas também regenera os pacotes de dados antes de encaminhá-los para a porta de saída

- **Reconfiguração de pacotes:** O TAP ativo é capaz de reconfigurar pacotes e reconstituir o sinal elétrico, permitindo a compensação de atrasos no tráfego e melhorando a qualidade do sinal.
- **Filtragem de tráfego:** O TAP ativo pode incluir recursos adicionais, como filtragem de tráfego, que permite selecionar quais pacotes de dados serão copiados e enviados para a porta de saída, tornando-o mais flexível em ambientes de alta velocidade e alta densidade de tráfego.

5.3 User and Entity Behavior Analytics (UEBA)

É uma abordagem avançada de análise de segurança cibernética que utiliza algoritmos de aprendizado de máquina e técnicas de análise comportamental para identificar atividades incomuns, suspeitas ou maliciosas relacionadas a usuários e entidades em um ambiente de rede. **O objetivo do UEBA é detectar ameaças internas e externas que possam passar despercebidas pelas abordagens tradicionais de segurança**.

Funcionamento:

- **Coleta de dados:** O UEBA coleta dados de diferentes fontes em toda a rede, como logs de eventos de sistemas, registros de autenticação, registros de acesso a aplicativos, atividades de usuários, dados de tráfego de rede e informações sobre entidades (por exemplo, servidores, dispositivos, aplicativos).
- **Criação de perfis de comportamento:** Com base nos dados coletados, o UEBA cria perfis de comportamento normais para usuários e entidades. Esses perfis descrevem os padrões típicos de comportamento de cada usuário e entidade, levando em consideração suas funções, horários, padrões de acesso a aplicativos, entre outros fatores.
- **Aprendizado de máquina:** O UEBA utiliza algoritmos de aprendizado de máquina e análise estatística para aprender com os dados históricos e identificar padrões sutis e relacionamentos entre eventos. Esses algoritmos são treinados para reconhecer comportamentos normais e anormais com base nas informações coletadas.
- **Detecção de anomalias:** Quando um evento ou atividade é detectado pelo UEBA, o sistema compara essa atividade com os perfis de comportamento normais. Se a atividade se desviar significativamente do comportamento típico, ela é considerada uma anomalia.
- **Avaliação de riscos:** Além de identificar anomalias, o UEBA avalia o risco associado a cada evento detectado. Ele considera a gravidade da anomalia, o contexto da atividade, a sensibilidade dos dados envolvidos e outros fatores relevantes para determinar o nível de risco associado.
- **Geração de alertas:** Quando uma anomalia de alto risco é identificada, o UEBA gera alertas em tempo real para notificar os administradores de segurança sobre a atividade suspeita. Esses alertas permitem que os administradores investiguem e respondam rapidamente a possíveis ameaças.
- **Melhoria contínua:** O UEBA é um processo de aprendizado contínuo. À medida que o sistema coleta mais dados e é exposto a novos comportamentos, ele continua a

aprimorar seus modelos e a melhorar a precisão na detecção de ameaças e comportamentos anômalos.