**Firewall**

Quanto mais segurança menos praticidade!!

Existem os firewalls pessoais e de rede no qual podem ser de nível de aplicação ou de filtragem de pacotes

Ter tanto o firewall de rede e o pessoal se tornar melhor, pois tendo só o firewall de rede você pode sofrer um ataque interno pois nem sempre toda ameaça vem da internet , por exemplo dentro do INATEL um pc pode sofrer ataques de outro pc dentro do INATEL no qual o firewall nem saberá dessa ação maliciosa pois ele só toma conhecimento por trafego passado por ele

**No firewall existe 2 regras:**

**Regras de Entrada**: Filtra os pacotes que entra na maquina

**Regra de Saída**: Filtra os pacotes que sai da maquina

**Os firewalls já vêm com políticas padrões para tomada de decisão:**

**Descartar** (Aquilo que não é expressamente permitido é proibido = se eu não expressei permitindo um determinado acesso, aquele acesso já proibido, então isso já vem por padrão e vamos habilitando as permissões de acesso como exemplo de jogo abaixo)

**Encaminhar** (Aquilo que não é expressamente proibido é permitido)

Tipos de regras:

Programa, Porta (TCP ou UDP), predefinida ou personalizada

Se caso o firewall bloquear a comunicação com um servidor de um jogo especifico ( política padrão descartar do firewall), não é recomendado aparar o firewall , e sim criar um regra especifica para o programa/jogo na hora que entrasse no jogo ele habilitava a regra no firewall podendo jogar em problemas e continuava seguro com o firewall filtrando as outras coisas

Por um bloquei por porta, por exemplo caso bloquei o TCP dando como porta especifica a porta **80** (porta padrão pra acesso HTTP) e bloquear a conexão então agora toda vez que tentar fazer um acesso HTTP o firewall irá barrar

Também pode bloquear um IP especifico

(HTTP + TLS = HTTPS = porta 443)

Pelo firewall não é somente bloquear uma conexão, mas também tem a opção de permitir

Normalmente os firewalls de filtragem de pacotes trabalham:

-Camada de transporte Control Protocol (TPC)

-Internet Protocol (IP)

-Data Link

-Physical

E também nos firewalls atualmente nas Aplicações, pois independente se os firewalls são de rede ou pessoal, eles podem ser de nível de aplicação

**Firewall de aplicação (ALG) vantagens:**

- Tendem a ser mais seguros (**isso não quer dizer que são mais seguros**, mas que tender a ser mais seguros por causa da facilidade que se tem para fazer as configurações do firewall por exemplo se comparar um firewall ALG com um firewall de filtragem de pacotes bem configurado os dois **são igualmente seguros** )

- Não é necessário explorar todas combinações dos filtros de pacote

- Somente examina algumas aplicações permitidas

- Fácil registrar e auditar todo o trafego

**Firewall de aplicação (ALG) desvantagens:**

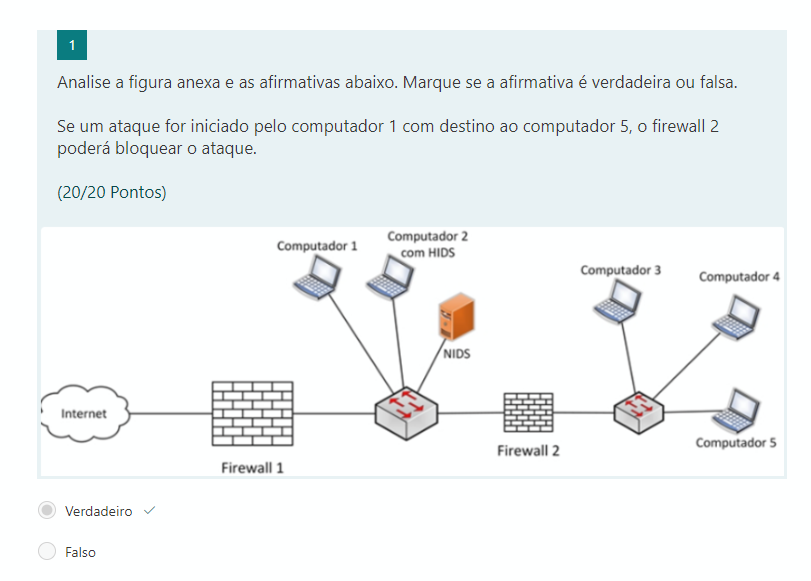
Overhead de processamento adicional em cada conexão (em cada sessão que eu abro de dentro da minha rede ou de fora eu tenho um processamento adicional no sistema = processamento para ler as informações da camada de aplicação) então a rede tende a ficar mais lenta devido a latência adicional promovida pelo firewall

O firewall de filtragem de pacote é mais complicado de configurar (se não toma cuidado se pode deixa muitas brechas no firewall

O firewall de nível de aplicação é mais fácil de configurar e ele tende a ser mais seguro porem tem a desvantagem da latência de rede ao aplicar

Para resolver esses problemas sita acima foi criado o Firewall de inspeção com estado (ele é um ALG ) quando tenta fazer um acesso e passa pelo firewall ele analise por exemplo ele ver que o HTTP é permitido então ele permiti o acesso a esse site então ele cria uma regra de filtragem e uma segunda regra de filtragem (para o trafego esperado pois se foi feito uma requisição ira ter uma resposta) só que agora ele não precisa analisar todos os pacotes da resposta em nível de aplicação só o primeiro diminuindo o overhead

Tarefa Firewall



1 - Se um ataque externo for direcionado ao computador 3 e, esse ataque, conseguir passar pelo firewall 1, certamente ele será bloqueado pelo firewall 2**. (Falso)**

2 - Se um ataque se iniciar na Internet e tiver como destino o computador 3, tanto o firewall 1 quanto o firewall 2 poderão bloquear tal ataque. **(Verdadeiro)**

3 - Se um ataque se iniciar na Internet e tiver como destino o computador 1, o firewall 1 poderá bloquear o ataque, porém, o firewall 2 não poderá bloqueá-lo. (20/20 Pontos) **(Verdadeiro)**

4 - O firewall 1 é um firewall de rede enquanto que o firewall 2 é um firewall pessoal. Sendo assim, é correto afirmar que o firewall 1 será um firewall de nível de aplicação e o firewall 2 será um firewall de filtragem de pacotes **(Falso)**

**IDS e IPS**

Nem tudo dá pra ser resolvido com firewall então ao longo dos anos foi desenvolvido outras ferramentas e uma delas de sucesso foi o IDS e IPS

1. -Funciona como um alarme (tem a opção de quando acontecer o alarme, bloquear o trafego que ocorreu o alarme)
2. - Gera o alarme com base de 2 tipos de conhecimento:

* --Assinatura de ataques (existe um vírus especifico q tem um ataque especifico que já foi mapeado, porém não funcionaria em novos ataques)
* --Aprendizado de uma rede neural (aprende as utilizações normais da rede, levanta as estatísticas daquela rede ao longo de muito tempo, então ele aprende o comportamento padrão da rede então tudo que foge do padrão pode ser detectado como uma ameaça

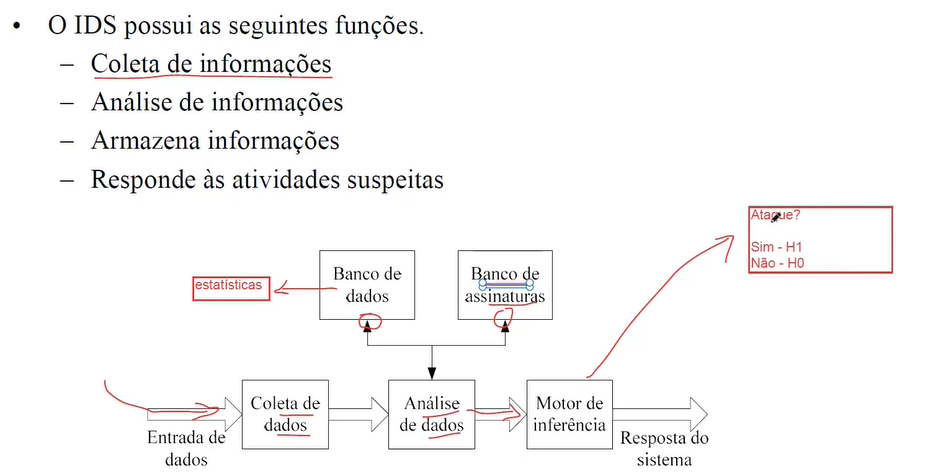
1. Existe basicamente dos tipos de IDS:

* NIDS (IDS de Rede)
* HIDS (IDS de host)

**Funções do IDS**

* Coleta de informações (os pacotes que estão passando na rede, os tipos, podendo coletar dados por usuário/IP coletando dados do daquele usuário)

Coleta os dados , analisa os dados e faz uma comparação entre as informações que ele já tem na base de dados(guarda as estatísticas, vazão media da rede em um horário , uso de processamento dos roteadores em um horário , número de acessos em u horário ) e no banco de assinatura( assinaturas dos ataques já conhecidos) e monta uma resposta do sistema apenas sim ou não (binaria)



**Resultados possíveis de uma analise**

H0: Não está sobre ataque

H1: Está sobre ataque

* **Trafego suspeito detectado (comportamento normal)**

**H1 | H1: IDS Decidiu H1 dado por esta em condição de H1**

* Trafego suspeito não detectado (Falso negativo)

H0 | H1: IDS fala que estava sobre H0 porem estava em H1

* Trafego legitimo que o IDS analisa como sendo suspeito (falso positivo)

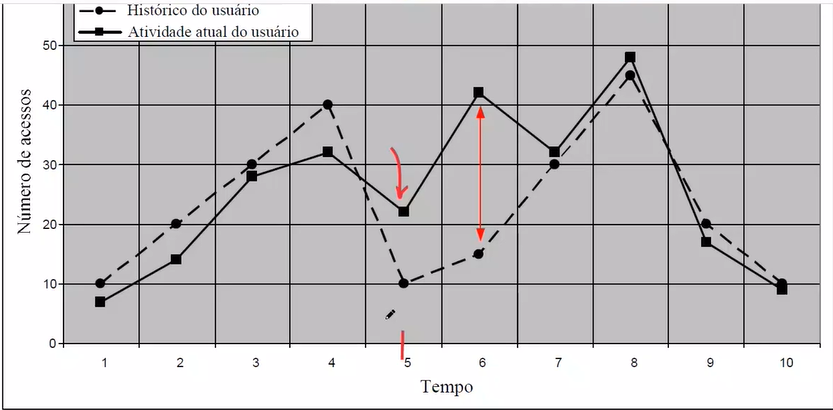
H1| H0: IDS fala que estava sobre H1 porem estava em H0

Problema de gerar falso positivo que gera uma falta de credibilidade no IDS, então após várias ocorrências a pessoa pode desligar o alarme ao invés de checar a causa do alarme como um alarme de carro que sempre pensamos que não é nada quando corre

* **Trafego legitimo que o ID analisa como sendo normal (comportamento normal)**

**H0 | H0: Estando em H0 toma a decisão H0**

Com duas formas acima já da pra saber se a IDS é boa o mais usado é a primeira quanto trafego suspeito ele detecta (probabilidade de detecção) e a terceira quanto ele é bom em perceber trafego legitimo sem que soa o alarme de ataque (probabilidade de falso alarme)

Gráfico de acesso de um usuário/IP: 

No caso eteve uma diferenca muito grande acesso em um horario especifico

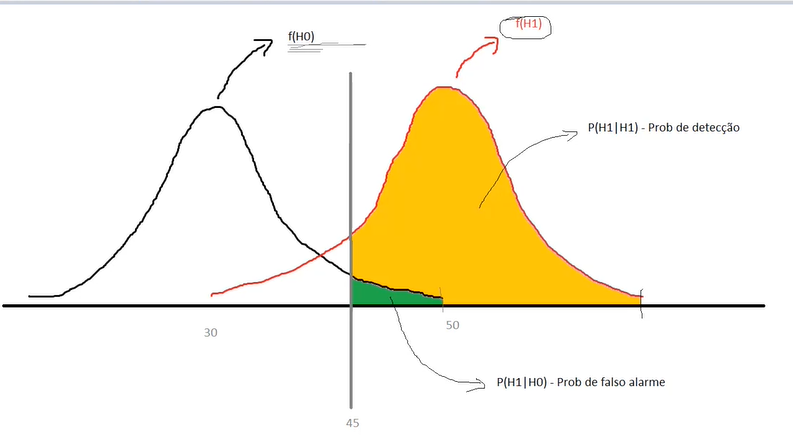
Mas isso pode não ser um ataque pode ser so um usuario trabalhando correndo em horario de almoco , nesse caso mostra como pode ser ruim deixa o proprio IDS toma a decisao após um alarme , imagina que for so isso de um usuario tentando adiantar algo na hora do almoco e seu computador é bloqueado/ deslidado, por isso é bom deixa a IDS por muito tempo apenas com o alarme após muito tempo e confiança que deixa ele aplicar decisões em cima dos alarmes gerados

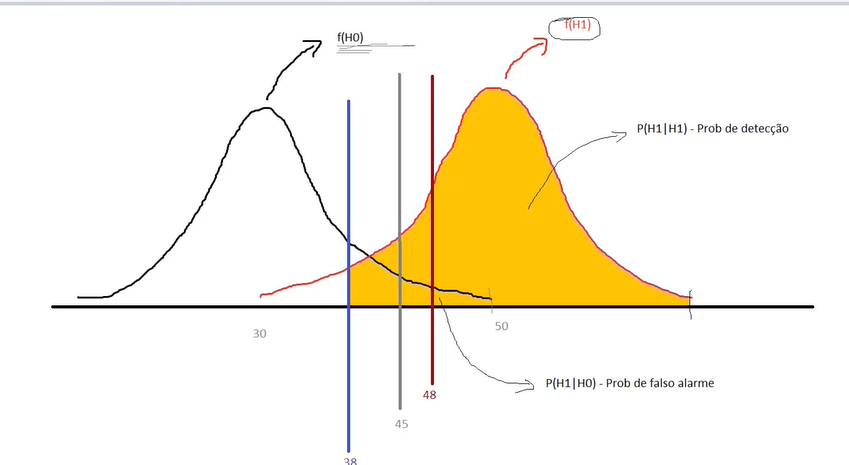
2 estatísticas guardado no banco de dados

f(H0): Quando não está sobre ataque (media 30 acessos)

f(H1): Quando está sobre ataque (media 50 acesos)

vendo isso toma um linear de decisão para os IDS (linha vertical) (media 45 acessos):



Como pode ser visto abaixo a mudança na linear de decisão ira variar tanto probabilidade de detecção quanto a de falso alarme , quanto mais área de (H1|H1) mais falso alarme será gerado (H1|H0) , porem quanto menos (H1|H0) menos detecção de ataque real (H1|H1): 

Não existe um ponto otimo podento ter o falso alarme como referencia dizendo por exemplo que aceita ate 15 % de falso alarme sem que o IDS perca a credibilidade