Análise da Informação
Manuel Martins

d /concursos

SEGURANÇA DA INFORMAÇÃO

FERRAMENTAS DE SEGURANÇA

✓FIREWALL ⇒ são barreiras interpostas entre a rede privada da organização e a rede externa. São baseados na **combinação** de **hardware** e **software** ou **somente** em **software**. O firewall analisa o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com as regras definidas previamente.

FERRAMENTAS DE SEGURANÇA

✓FIREWALL ⇒ É o principal instrumento de defesa de uma rede corporativa já que centraliza a administração e a configuração de segurança, dispensando a instalação de softwares adicionais em cada host (máquina) da rede.

REGRA BÁSICA DE UM FIREWALL é: **O QUE NÃO FOR EXPRESSAMENTE PERMITIDO É PROIBIDO**.

FERRAMENTAS DE SEGURANÇA

O QUE O FIREWALL NÃO PROTEGE

- ✓ ATAQUES INTERNOS DE USUÁRIOS MAL INTENCIONADOS ⇒ o firewall analisa e protege o tráfego entre duas redes. Assim, se um usuário mal intencionado estiver acessando a rede da organização internamente, poderá não passar pelo firewall, e se tentar efetuar algum ataque poderá ter êxito.

FERRAMENTAS DE SEGURANÇA

O QUE O FIREWALL NÃO PROTEGE

- ✓ PROTEÇÃO ANTIVÍRUS ⇒ o firewall não protege a rede interna contra a infecção de vírus, cavalos de Tróia e outras pragas virtuais, sejam eles decorrentes de downloads, e-mails atachados ou outras formas de infecção. A utilização de um **ANTIVÍRUS** é indispensável.

FERRAMENTAS DE SEGURANÇA

O QUE O FIREWALL NÃO PROTEGE

✓PORTAS ABERTAS OU BACKDOORS ⇒ para que o funcionamento do firewall seja eficiente é necessário que não existam backdoors, ou portas dos fundos abertas. Por exemplo, se todo acesso da organização à Internet é feito através de um firewall, que possui uma série de regras pré-definidas, e houver estações que utilizem modem para acessar a Internet, esse acesso não estará sendo feito pelo firewall e portanto não estará sujeito as restrições, podendo tornar a rede interna vulnerável a intrusões.

FERRAMENTAS DE SEGURANÇA

O QUE O FIREWALL NÃO PROTEGE

✓**BUGS E FALHAS NO EQUIPAMENTO** ⇒ falhas no equipamento ou uma má configuração, podem deixar o firewall indisponível por um tempo suficiente para um intruso invadir a rede interna da organização.

✓**COLISÕES DA REDE INTERNA E EXTERNA** ⇒ colisões da rede interna e externa podem evitar o acesso ao firewall por alguns instantes. Isso pode ser aproveitado por um intruso para invadir a rede interna, roubando informações ou deixando algum código hostil, que abra backdoors para um ataque a rede posteriormente.

FIREWALL - FILTRAGEM DE PACOTES

✓A filtragem de pacotes é feita, em geral, com a utilização de um roteador de filtragem de pacotes projetado para filtrar à medida que eles passam entre as interfaces do roteador.

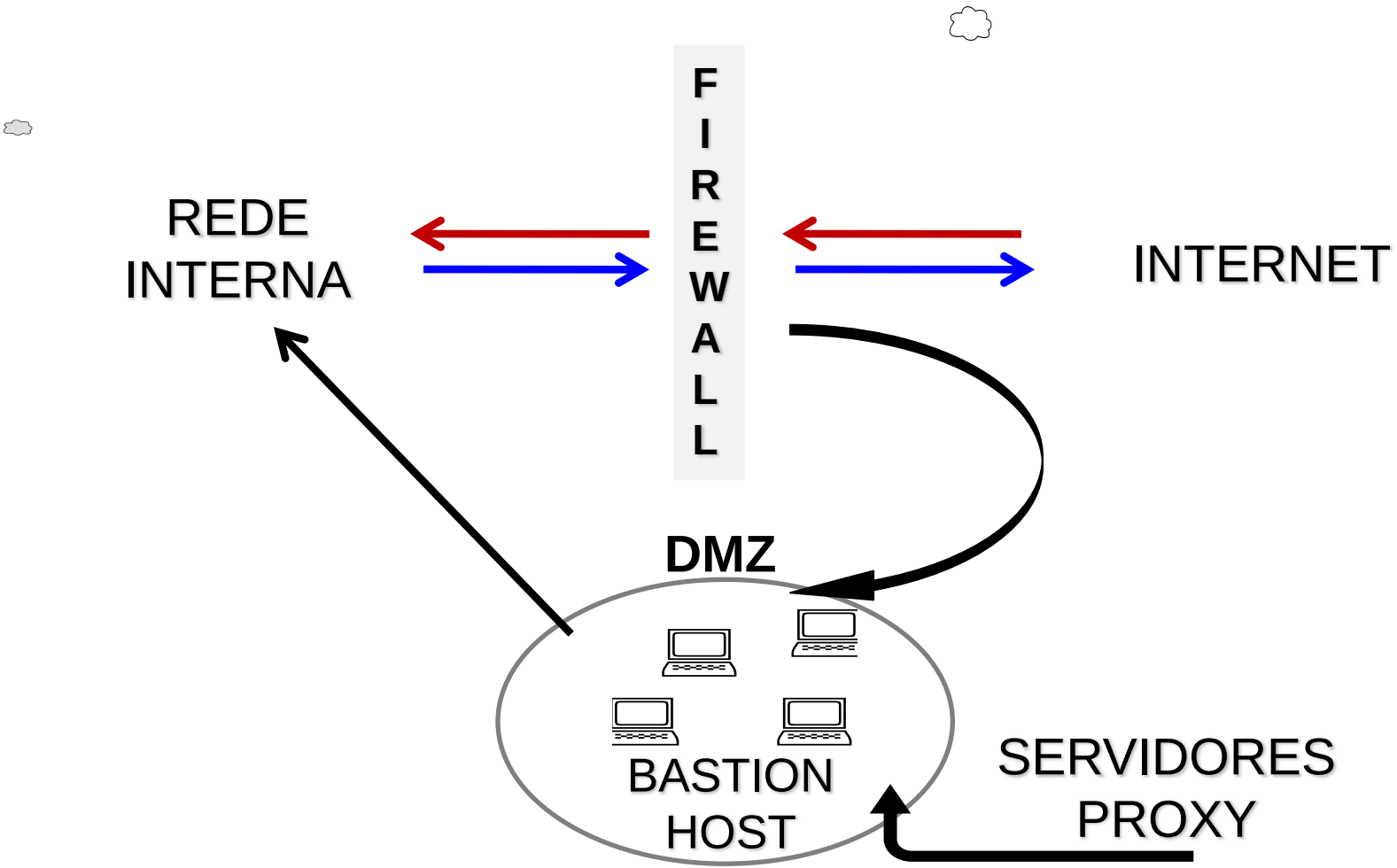
✓A filtragem de pacotes é feita através dos seguintes campos:

- ENDEREÇO IP DE ORIGEM
- ENDEREÇO IP DE DESTINO
- PORTA DE ORIGEM TCP/UDP
- PORTA DE DESTINO TCP/UDP

FERRAMENTAS DE SEGURANÇA

- ✓DMZ (*De-Militarized Zone*) ⇒ É uma rede posicionada entre uma rede protegida (rede interna) e uma rede externa, para proporcionar um nível adicional de segurança a seus sistemas internos e usuários. Na DMZ, conhecida também como **REDE DE PERÍMETRO**, normalmente residem máquinas que provêem serviços ao público externo, como: Servidores Proxy, Servidores Web, DNS, etc.

FERRAMENTAS DE SEGURANÇA - DMZ



FERRAMENTAS DE SEGURANÇA

- ✓IDS (Intrusion Detection System) ⇒ Um software que **mapeia** e **detecta tentativas** de **invasão** a **uma rede** de computadores. Na maioria das vezes **não bloqueia** uma **ação**, mas **verifica** se a **ação é ou não uma ameaça** para um segmento de rede. Como complemento do IDS, temos o **IPS** (**Intrusion Protection System**), que tem a capacidade de identificar uma intrusão, analisar a relevância do evento/risco e bloquear determinados eventos, fortalecendo assim a técnica de detecção de intrusos.

TIPOS DE IDS

- ✓HOST BASED (HBIDS)
- ✓NETWORK BASED (NIDS)
- ✓HIDS (HYBRID IDS)

FERRAMENTAS DE SEGURANÇA

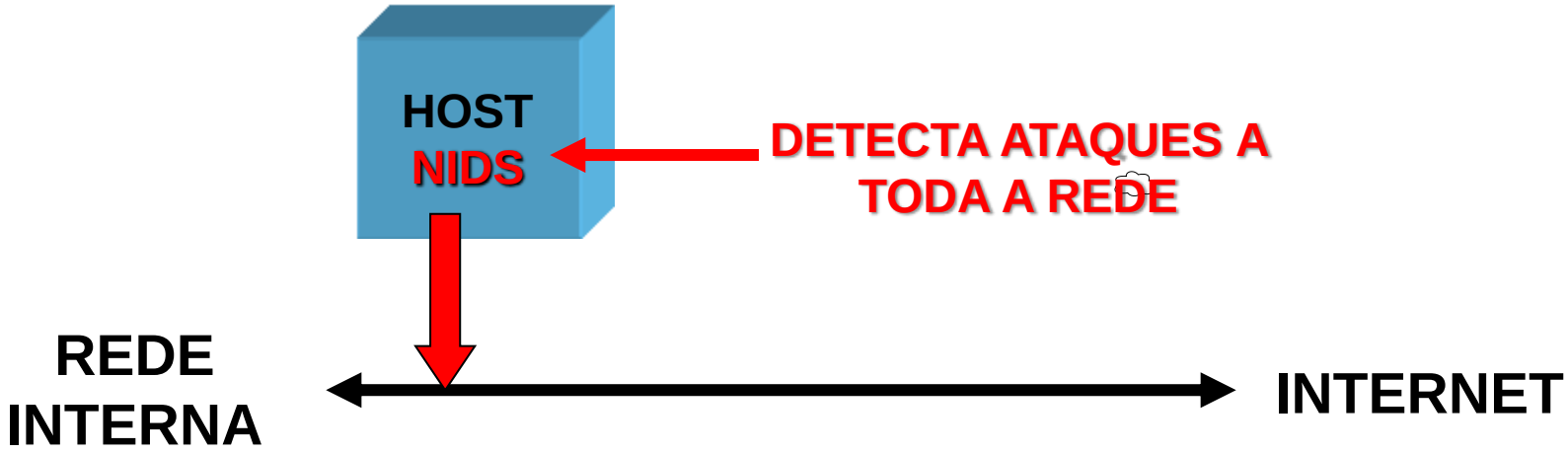
- ✓HOST BASED (HBIDS) ⇒ são instalados em um servidor para alertar e identificar ataques e tentativas de acessos indevidos **à própria máquina**. São avaliados vários aspectos da segurança do servidor como: arquivos de logs do Sistema Operacional, logs de aplicação, logs de acesso.

FERRAMENTAS DE SEGURANÇA

- ✓NETWORK BASED (NIDS) ⇒ são instalados em máquinas que serão responsáveis por identificar ataques **direcionados** a **toda** a **rede**, por meio da monitoração do tráfego. Assim, um NIDS é, essencialmente, um **sniffer** (**farejador**) que captura pacotes na rede e compara com uma base de assinaturas de ataques (são um conjunto de comandos que pertencem a um ataque específico), gerando alertas. Essa informação é enviada para o administrador da rede ou administradores de segurança, como uma suposta tentativa maliciosa.

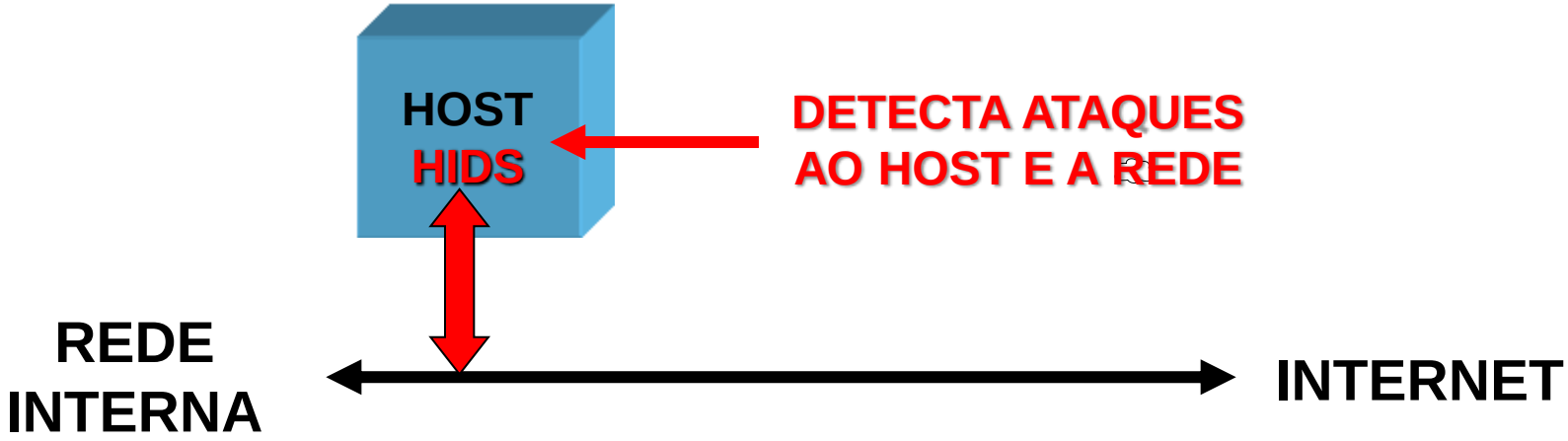
FERRAMENTAS DE SEGURANÇA

✓NIDS ⇒ NETWORK BASED



FERRAMENTAS DE SEGURANÇA

- ✓HIDS (*Hybrid* IDS) ⇒ junta o HBIDS e NIDS em uma só ferramenta.



FERRAMENTAS DE SEGURANÇA

✓IDS ⇒ TIPOS DE ERRO

- FALSO POSITIVO ⇒ ocorre quando a ferramenta **classifica** uma **ação** como uma **possível intrusão**, quando na verdade **trata-se** de uma **ação legítima**.
- FALSO NEGATIVO ⇒ ocorre quando uma **intrusão real acontece** mas a ferramenta a **classifica** como uma **ação legítima**.
- ERRO DE SUBVERSÃO ⇒ ocorre quando uma **ferramenta** de IDS é **modificada** pelo **intruso** para **forçar** a ocorrência de **falso negativo**.

FERRAMENTAS DE SEGURANÇA

- ✓**IPS** (Intrusion Prevention System) ⇒ funciona como um IDS que consegue detectar e bloquear ataques, ou seja, identifica e atua sobre atividades anômalas de rede sendo assim um **elemento ativo**. A **diferença** entre **IDS** e **IPS** está no fato de que, enquanto os **IDSs agem somente após** a **ocorrência** da **intrusão**, **como** um **alarme** que **detecta** a **presença** de um **invasor**, os **IPSs** foram desenvolvidos como **medidas** de **prevenção**, ou seja, para **bloquear possíveis ataques antes** que eles **tenham sucesso**, ou pelo menos para limitar suas conseqüências negativas, caso venham a ocorrer.

FERRAMENTAS DE SEGURANÇA

✓ SCANNERS DE VULNERABILIDADES (PORT SCAN) ⇒ softwares que **varrem** as **portas** utilizadas pelo protocolo TCP/IP, com o **objetivo** de **detectar vulnerabilidades** nas portas utilizadas pela rede. Podem obter informações como:

- serviços que estão sendo utilizados;
- usuários que utilizam estes serviços;
- possibilidade de conexão por usuários anônimos;
- possibilidade de conexão por usuários sem autenticação.

FERRAMENTAS DE SEGURANÇA

- ✓HONEYPOT ⇒ é um recurso computacional de segurança de rede dedicado a ser sondado, atacado ou comprometido.

TIPOS DE HONEYPOT

- HONEYPOTS DE BAIXA INTERAÇÃO (Low-interaction Honeypots)
- HONEYPOTS DE ALTA INTERAÇÃO (High-interactionHoneypots)

FERRAMENTAS DE SEGURANÇA

- ✓HONEYPOTS DE BAIXA INTERAÇÃO ⇒ normalmente apenas emulam serviços e sistemas operacionais, **não permitindo** que o **atacante interaja** com o **sistema**.
- ✓HONEYPOTS DE ALTA INTERAÇÃO ⇒ são compostos por sistemas operacionais e serviços reais e **permitem** que o **atacante interaja** com o **sistema**.

FERRAMENTAS DE SEGURANÇA

✓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 e controle eficientes e transparentes, para que não seja usada como origem de ataques a outras redes. Uma HoneyNet deve ser **projetada** também para **não alertar** o **invasor** de que ele está em uma HoneyNet.

FERRAMENTAS DE SEGURANÇA

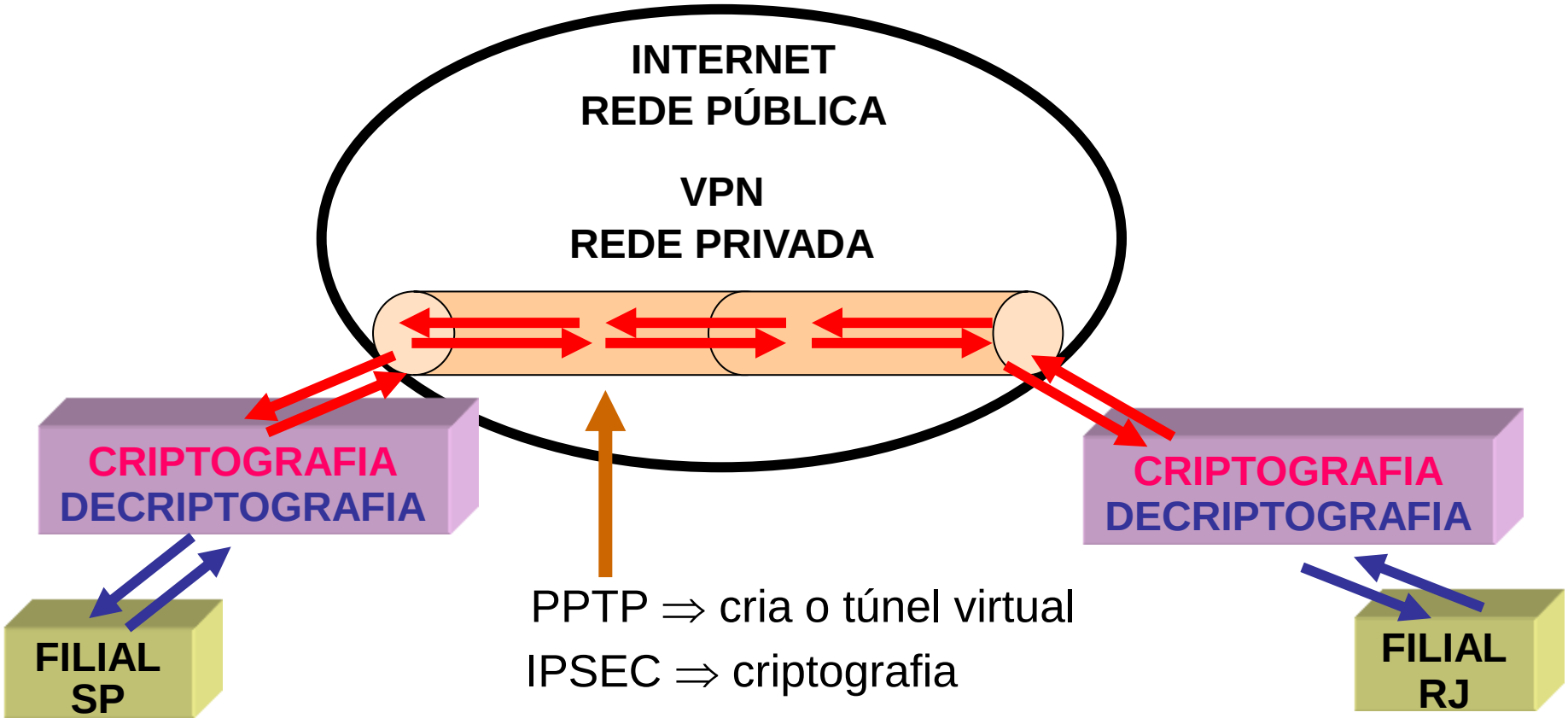
- ✓VPN (Virtual Private Network) ⇒ rede **particular** que utiliza a infra-estrutura de uma rede **pública** de telecomunicações, como a Internet, por exemplo, para a transmissão de **informações confidenciais**. Os dados transmitidos são **encriptados**. Sua implementação se dá por meio de firewalls instalados entre as redes particulares e a Internet, formando túneis virtuais pelos quais trafegam as informações, protegendo-as do acesso de usuários não autorizados.

FERRAMENTAS DE SEGURANÇA

- ✓Este tipo de rede é mais empregado no âmbito corporativo, conectando a matriz às suas filiais espalhadas em diferentes cidades ou países. Alguns protocolos utilizados no túnel virtual, são:

  PPTP (Point-to-Point Tunneling Protocol) e o **IPSec** (Internet Protocol Security).

VPN (VIRTUAL PRIVATE NETWORK)



✓PPTP (Point to Point Tunneling Protocol) ⇒ é um protocolo de **encapsulamento** ponto a ponto que permite encapsular pacotes **PPP** (Point to Point Protocol) dentro de pacotes IP e encaminhá-los através de qualquer rede IP, incluindo a própria Internet. É um dos protocolos utilizado em uma **VPN** (Virtual Private Network). Porta 1723. Camada de Enlace (2).

OUTROS PROTOCOLOS DE TUNELAMENTO ⇒ L2TP e L2F

- ✓IPSEC (Internet Protocol Security) ⇒ é um conjunto de serviços de proteção baseados em criptografia e protocolos de segurança para **proteger** o **conteúdo** dos **pacotes IP** e assegurar a defesa contra ataques através da filtragem de pacotes e da aplicação de comunicações confiáveis. Fornece forte proteção contra ataques da Internet e de redes privadas (**VPN**) através da segurança ponto a ponto. Na comunicação, os únicos computadores que devem ter conhecimento sobre a proteção IPSec são o remetente e o receptor. Camada de Rede (3).

QUESTÕES DE PROVAS

01- (ACI-CGE-CE-CESPE-2019) - Para proteger a comunicação em uma organização que possui várias redes internas de computadores interligadas entre si e também à Internet contra ações maliciosas no tráfego dos dados, o mecanismo a ser utilizado é o

A) registro de logs.
B) antispam.
C) firewall.
D) antispyware.
E) controlador de domínio

GABARITO - C

(FUB-CESPE-2018) - Julgue os próximos itens, a respeito de segurança de redes.

02- Ocorre falso negativo quando um firewall bloqueia pacotes de dados de uma atividade legítima na rede por tê-la interpretado como maliciosa.

GABARITO - E

03- Em uma comunicação de rede, um **IPS** instalado em linha (no caminho de comunicação entre a origem e o destino) analisa ativamente o tráfego e pode disparar ações automatizadas em tempo real, como, por exemplo, bloquear o tráfego de uma origem identificada como maliciosa.

GABARITO - C

04- (FCC) - Uma subrede, que contém todos os serviços com acesso externo, localizada entre rede externa não confiável (Internet) e uma rede local confiável é

(A) um firewall baseado em filtros

(B) um sistema de detecção de intrusos

(C) um sistema de certificação digital

(D) uma zona desmilitarizada

(E) uma ferramenta de hardening

DMZ $\Rightarrow$ ZONA DESMILITARIZADA $\Rightarrow$ REDE DE PERÍMETRO

GABARITO - D

05- (FUNIVERSA-2016) Os protocolos de tunelamento que podem ser utilizados nas redes privadas virtuais (VPN) são:

Os protocolos de tunelamento que podem ser utilizados nas redes privadas virtuais (VPN) são

(A) IP, IPX e NetBEUI.
(B) IPSec, L2TP e PPTP.
(C) X25, Frame Relay e ATM.
(D) IP, IPX e ATM.
(E) IP, IPSec e X25.

GABARITO - B

06- (CFM-IADES-2018) - Port Scanner, Protocol Analyzer e Honeypots/Honeynets são ferramentas utilizadas no processo de:

(A) ameaças iminentes.
(B) análise de processos.
(C) análise de risco.
(D) análise de capacidade.
(E) análise de vulnerabilidade.

GABARITO - B

Carpe Diem