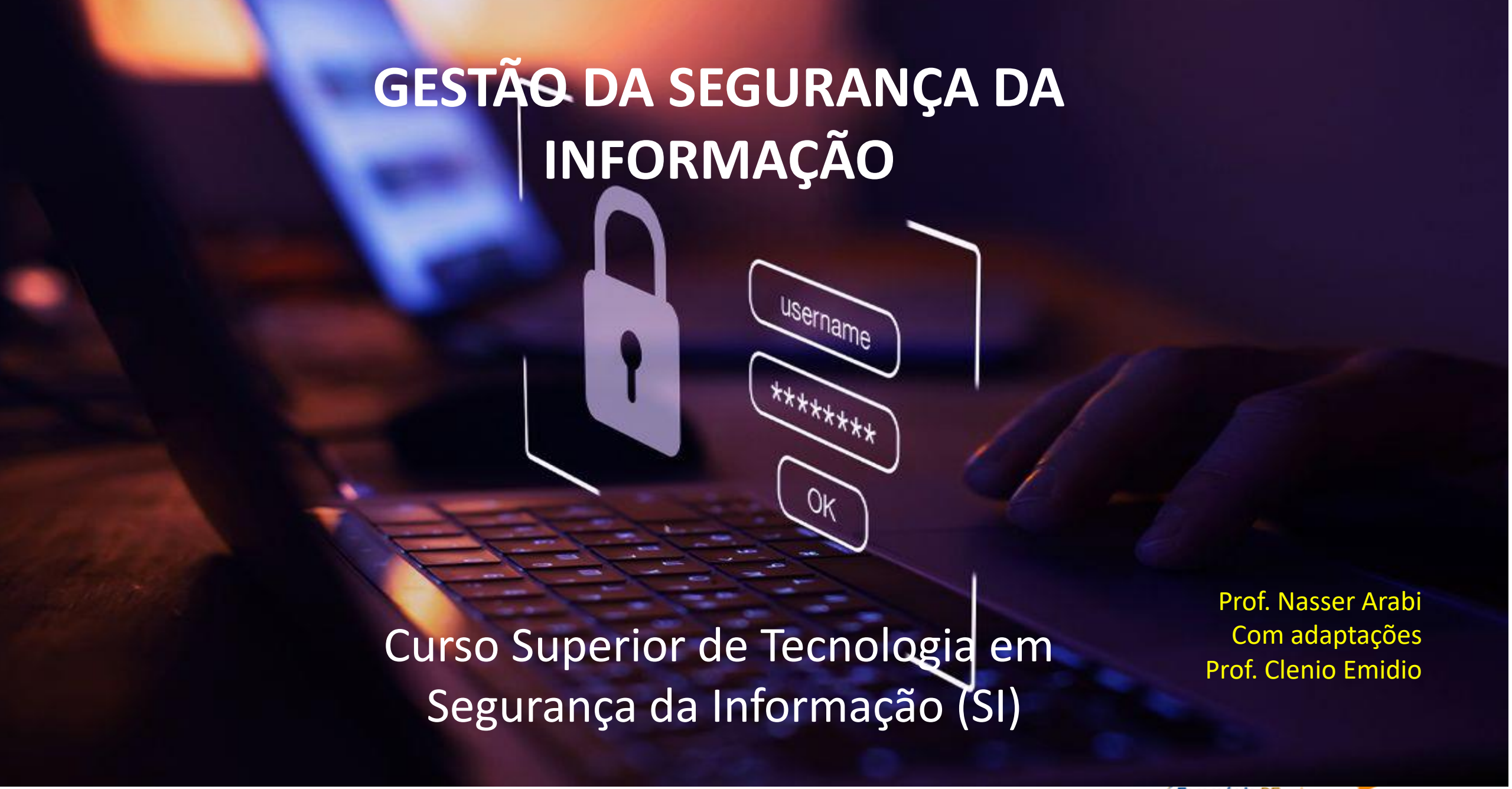
GESTÃO DA SEGURANÇA DA INFORMAÇÃO



Curso Superior de Tecnologia em Segurança da Informação (SI)

Prof. Nasser Arabi
Com adaptações
Prof. Clenio Emidio

Estratégias de proteção

Teoria do Perímetro

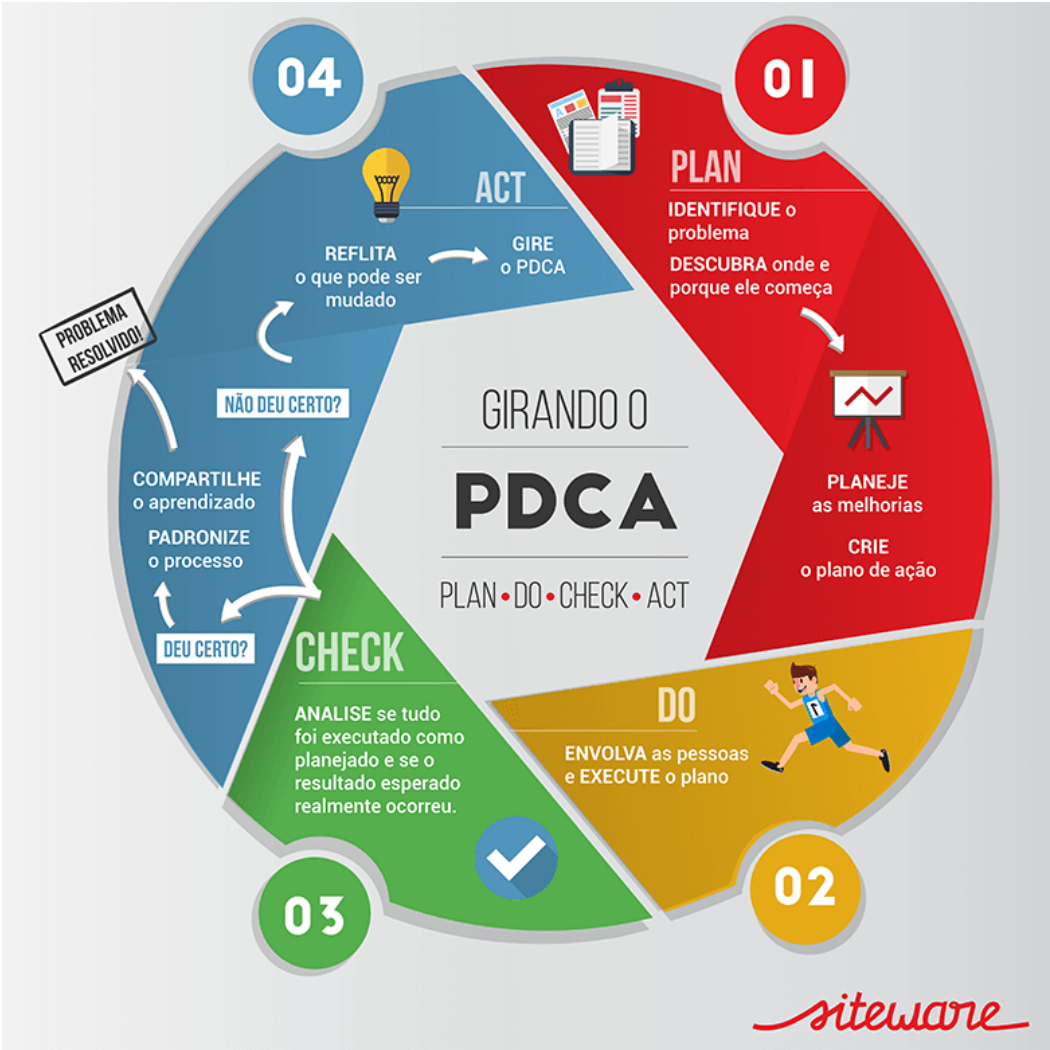
Teoria do Perímetro

A **teoria do perímetro** é a estrutura de segmentação de ambientes físicos, sendo considerada uma estratégia militar de defesa com o objetivo de assegurar os níveis de proteção da informação
A estratégia por trás dessa abordagem é simples e intuitiva: Se uma ameaça não consegue chegar até você (ou até o que você quer proteger), a segurança está garantida.
Esta proteção é uma necessidade emergente desde o início da humanidade, já retratada no período paleolítico. As pinturas primitivas, encontradas em cavernas, mostram esta como o primeiro abrigo seguro disponível.
Tal princípio também é utilizado com sucesso por outros seres vivos. A gaivota, por exemplo, constrói seu ninho nas encostas mais inacessíveis, longe de possíveis predadores.

Processo VIVO
e
DINÂMICO

Questões

- Como praticar a Segurança da Informação?
- Quais os modelos devem ser seguidos?
- Quais os mecanismos devem ser utilizados?
- Quais as ferramentas de segurança disponíveis e qual a melhor delas para cada caso?



Controle de acesso

"... tudo é proibido, exceto o que é expressamente permitido..."

Controle de acesso

- Classificação
  - Lógico: permissões em sistemas de arquivos, firewalls e perfis de usuário
  - Físico: portas, fechaduras e guaritas
  - Administrativo: políticas, normas e procedimentos
- Mecanismos
  - Desencorajador, limitador
  - Monitorador, detector
  - Preventivo, reativo, corretivo

Controles Lógicos

- Controle computacionais
  - Arquiteturas AAA (Autentication, Autorization, Accounting)
  - Antimalware: Antivirus, Antitrojan e Antispyware
  - Sistemas criptográficos simétricos e assimétricos
  - Hashes
  - Esteganografia
  - Certificação digital
  - Assinatura digital
  - Listas de controle de acesso
  - Automação de patching

Conceitos

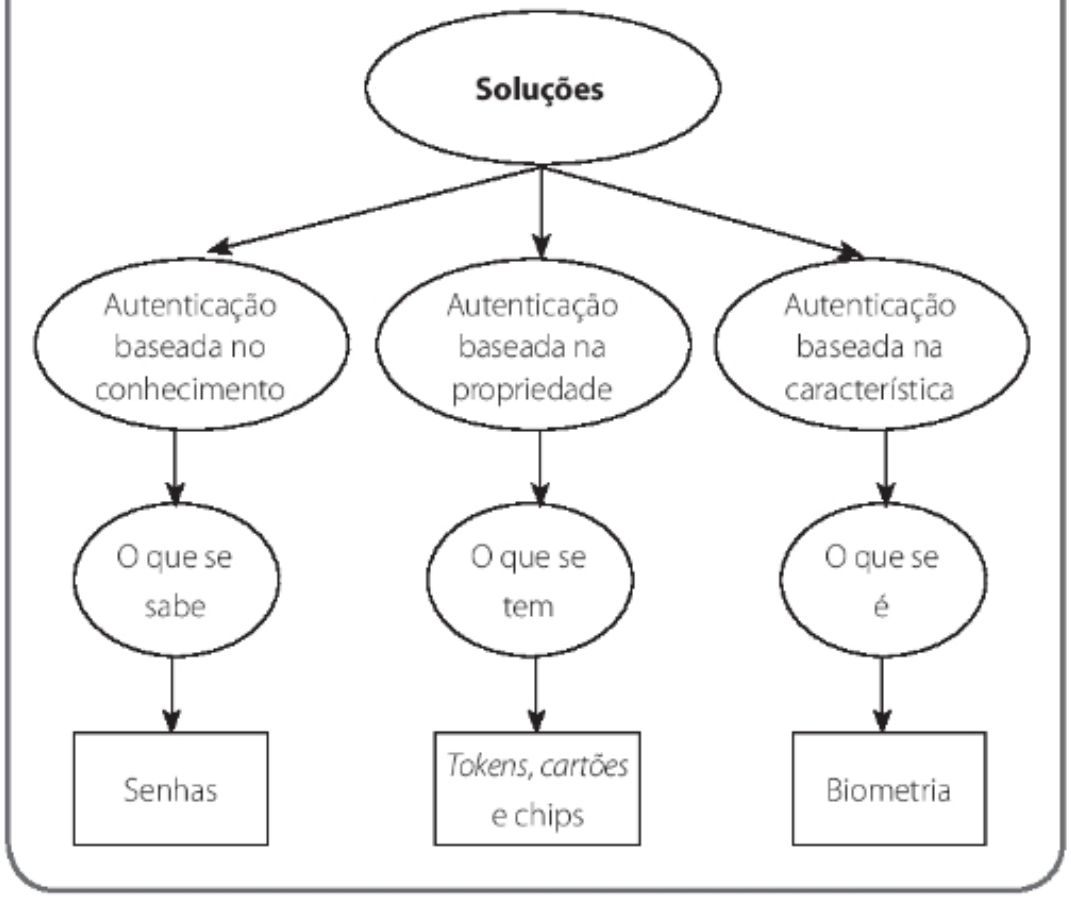
dentro de outra mensagem ou objeto físico para evitar a detecção. A esteganografia pode ser usada para ocultar praticamente qualquer tipo de conteúdo digital, incluindo texto, imagem, vídeo ou conteúdo de áudio. Esses dados ocultos são extraídos em seu destino.

Patching são programas que visam fazer correções de erros e bugs em softwares

Sistemas de identificação e autenticação de usuários

- Por conhecimento
- Por propriedade
- Por característica

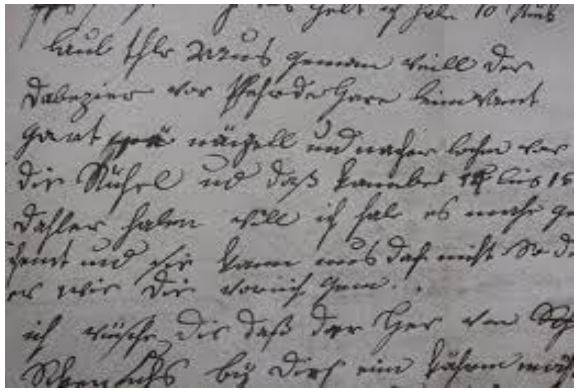
Figura 2.1 Tipos de autenticação de usuários e suas características.



Fundamentos em Segurança da Informação - Michele da Costa Galvão

Sistemas de identificação e autenticação de usuários

- Por conhecimento
  - perguntas randômicas;
  - senhas descartáveis.
- Por propriedade
  - token;
  - cartão;
  - crachá.
- Por característica
  - física e comportamental;
  - biometria;
  - escrita;
  - peso.



Controle de acesso à Informação (ISO 27002)

- **7 categorias de acesso:**

a) Requisitos de negócio para controle de acesso;
b) Gerenciamento de acesso do usuário;
c) Responsabilidades dos usuários;
d) Controle de acesso à rede;
e) Controle de acesso ao Sistema Operacional;
f) Controle de acesso à aplicação e à informação;
g) Computação móvel e trabalho Remoto.

Controle de Perímetro

- **O objetivo da segurança perimetral é a proteção contra ameaças externas.**

O tráfego de informações não só deve ser controlado, como pontos específicos desse tráfego devem ser identificados.

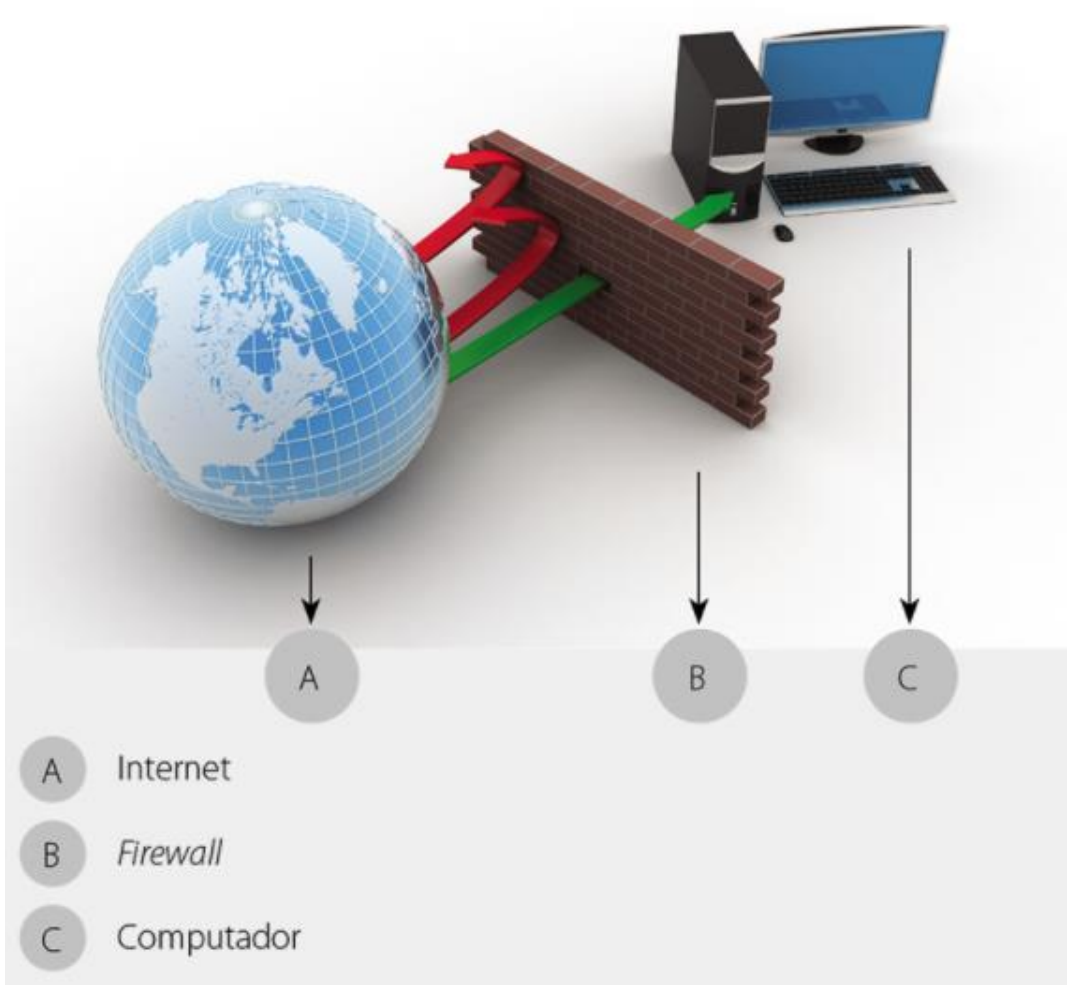
Quais pacotes de dados podem trafegar livremente e quais deverão ser bloqueados.

Controle de Perímetro

- Alguns mecanismos de proteção perimetral:
  - agentes proxy;
  - firewalls;
  - antivírus;
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - VPN
  - Unified Threat Management (Gerenciamento de Ameaças)
  - Security Information and Event Management
  - Switches Layer 7 – 802.1x e NAC
  - Blacklists

Firewall

- É uma junção de hardware e software aplicados em uma política de segurança que gerencia o tráfego de pacotes entre a rede local e a Internet em tempo real.



Tipos de Firewall

- Packet filtering (ou filtragem de pacotes) - lista de regras criadas; analisa se as informações são compatíveis, então aquele usuário é autorizado.
    - Estático
    - Dinâmico

- Proxy Services (ou firewall de aplicação) - não permite a comunicação direta entre origem e destino; todo o fluxo passe por ele; também executa tarefas complementares, como:
    - Registro de tráfego de dados em arquivo de log;
    - Armazenamento de conteúdos muito utilizados em cache;
    - Liberação de determinados recursos apenas mediante autenticação do usuário.

Tipos de Firewall

- Stateful Inspection (ou inspeção de estados) - fazem uma espécie de comparação entre o que está acontecendo e o que espera-se que aconteça; analisam todo o tráfego de dados em busca de padrões aceitáveis por suas regras,

* CISCO

- Firewall de proxy
- Firewall com inspeção de estado
- Firewall de Gerenciamento unificado de ameaças (UTM)
- Firewall de próxima geração (NGFW)
- NGFW focado em ameaças

https://www.antivirusguide.com/best-firewall/
https://www.cisco.com/c/pt_br/products/security/asa-5500-series-next-generation-firewalls/index.html

Sistema de descoberta e prevenção de intrusão

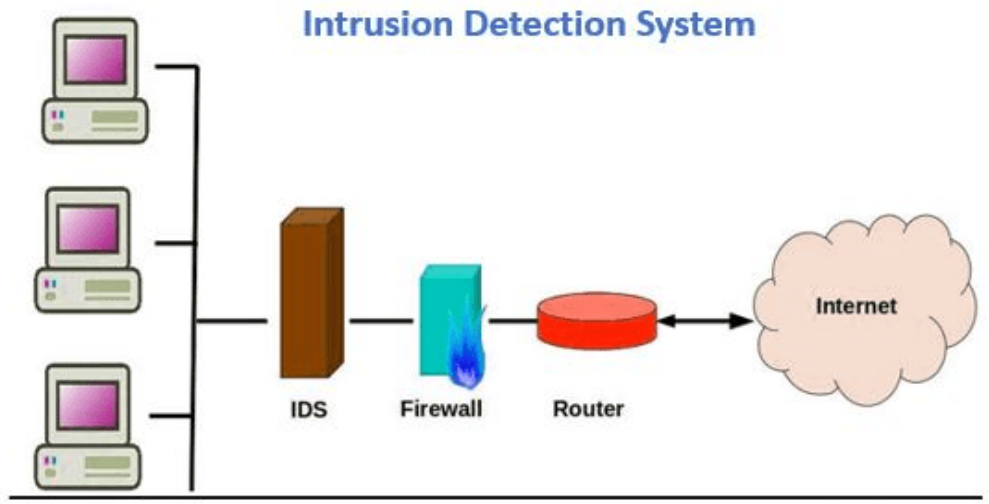
- Monitoramento de eventos “anormais” em sistemas computacionais, em rede ou no tráfego de rede.
- Varredura com o objetivo de encontrar rastros de intrusões ou possíveis incidentes:
    - acesso não autorizado às informações;
    - uso mal-intencionado de privilégios;
    - instalação de malware;
    - tentativas de obter privilégios não concedidos.

IDS - Intrusion Detection System e IPS- Intrusion Prevention System

infraestrutura de rede. Eles comparam pacotes da rede em um banco de dados de ameaças cibernéticas (que contém assinaturas conhecidas), e sinalizam todos os pacotes correspondentes.
A principal diferença entre eles é que o IDS é um sistema de monitoramento, enquanto o IPS é um sistema de controle de intrusão, que impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um

Sistema de descoberta e prevenção de intrusão

Intrusion Detection System (IDS) - Sistema de Detecção de Intrusão



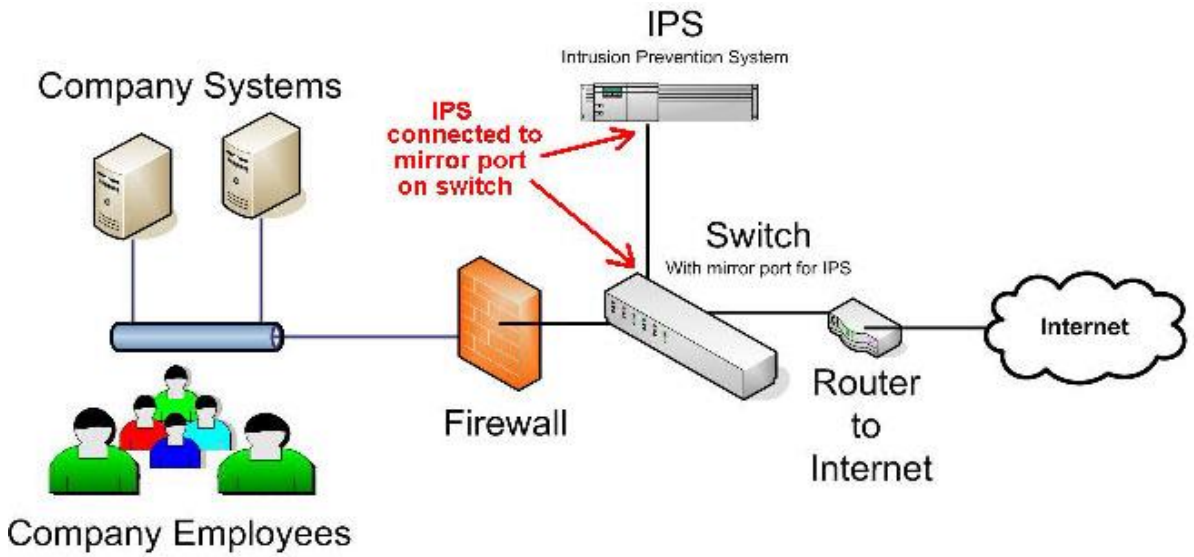
- coleta dados dos usuários e armazenando-os, analisando padrões comportamentais, fluxo de dados, horários, dentre outros;
- com essas informações, aliado ao conhecimento prévio de padrões de ataque, é possível discernir se o evento em questão é um evento malicioso ou não.
- configuração adequada – evitar falso positivo;

IDS

O **gerenciador de análise** é o cérebro do sistema. Ele consulta através de regras preestabelecidas o gerenciador de pacotes para efetuar uma eventual análise.
Se houver um pacote a ser analisado, o gerenciador de análise compara o pacote com as assinaturas requeridas ao gerenciador de assinaturas.
Caso haja confirmação das características do pacote serem descritas por alguma assinatura, o gerenciador de análise aciona o gerenciador de medidas de defesa para que seja combatida a ameaça detectada.
É assim que funcionam os sistemas de IDS. Eles analisam os registros de acesso à internet, procurando falhas que possam indicar uma invasão à rede, e sinalizam isso para que o administrador da rede possa agir ou entender o que está acontecendo.

Sistema de descoberta e prevenção de intrusão

Intrusion Prevention System (IPS) - Sistema de Prevenção de Intrusão



- impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um firewall impede o tráfego por endereço IP;
- nega proativamente o tráfego de rede com base em um perfil de segurança, se esse pacote representar uma ameaça de segurança conhecida.

Baseado em Host (HIDS)

Tipos de IDS e IPS

Sistema de Prevenção de intrusão baseado em rede (NIPS)

Sistema de Prevenção de intrusão baseado em host (HIPS)

Sistemas de Detecção de Intrusão Baseado em Rede (NIDS)

Ao invés de monitorar um único computador, o NIDS **monitora a rede como um todo**. Ele monitora o tráfego do **segmento** de rede no qual está inserido, com sua interface de rede atuando em modo indecoroso.
A detecção é feita através da captura e análise dos cabeçalhos e conteúdos dos pacotes, os quais são comparados com padrões ou assinaturas estabelecidas, sendo um mecanismo eficaz contra os ataques como: port *scanning*, IP spoofing, SYN *flooding*.
O uso de **múltiplos** NIDS em uma rede garante uma forma de defesa **abrangente**

Vantagens

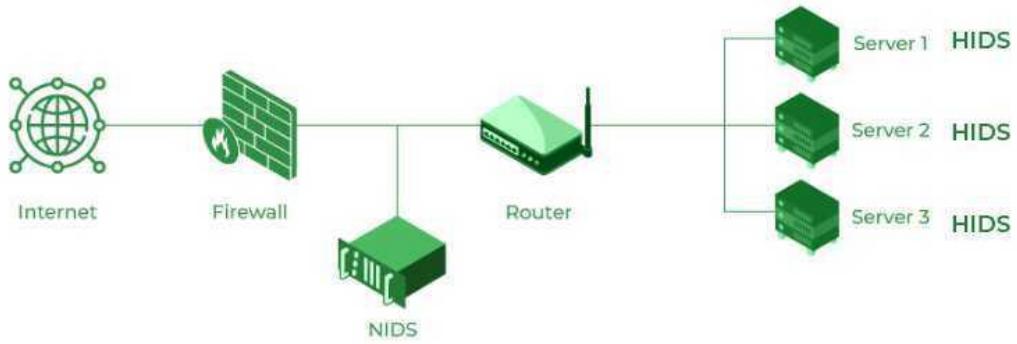
o desempenho da rede não é afetado; a detecção e identificação dos ataques é feita em tempo real, facilitando tomadas de decisões imediatas; eficácia na detecção de port scanning; não se restringe a somente detectar ataques, mas também às tentativas de ataque não concretizadas.

de defesa, no caso do ataque ter sido bem-sucedido e ter conseguido atravessar o firewall e o NIDS.

Sistemas de Detecção de Intrusão Baseado em Host (HIDS)

Com o HIDS é possível detectar as seguintes situações:

- Uso não correto e exagerado da memória;
- Processos cujo comportamento é suspeito Conexões suspeitas na rede;
- Utilização da CPU Utilização de System Calls;
- Uso detalhado do disco.



são tomadas decisões baseadas nas regras pré-definidas, e são essas regras que irão bloquear o ataque suspeito.

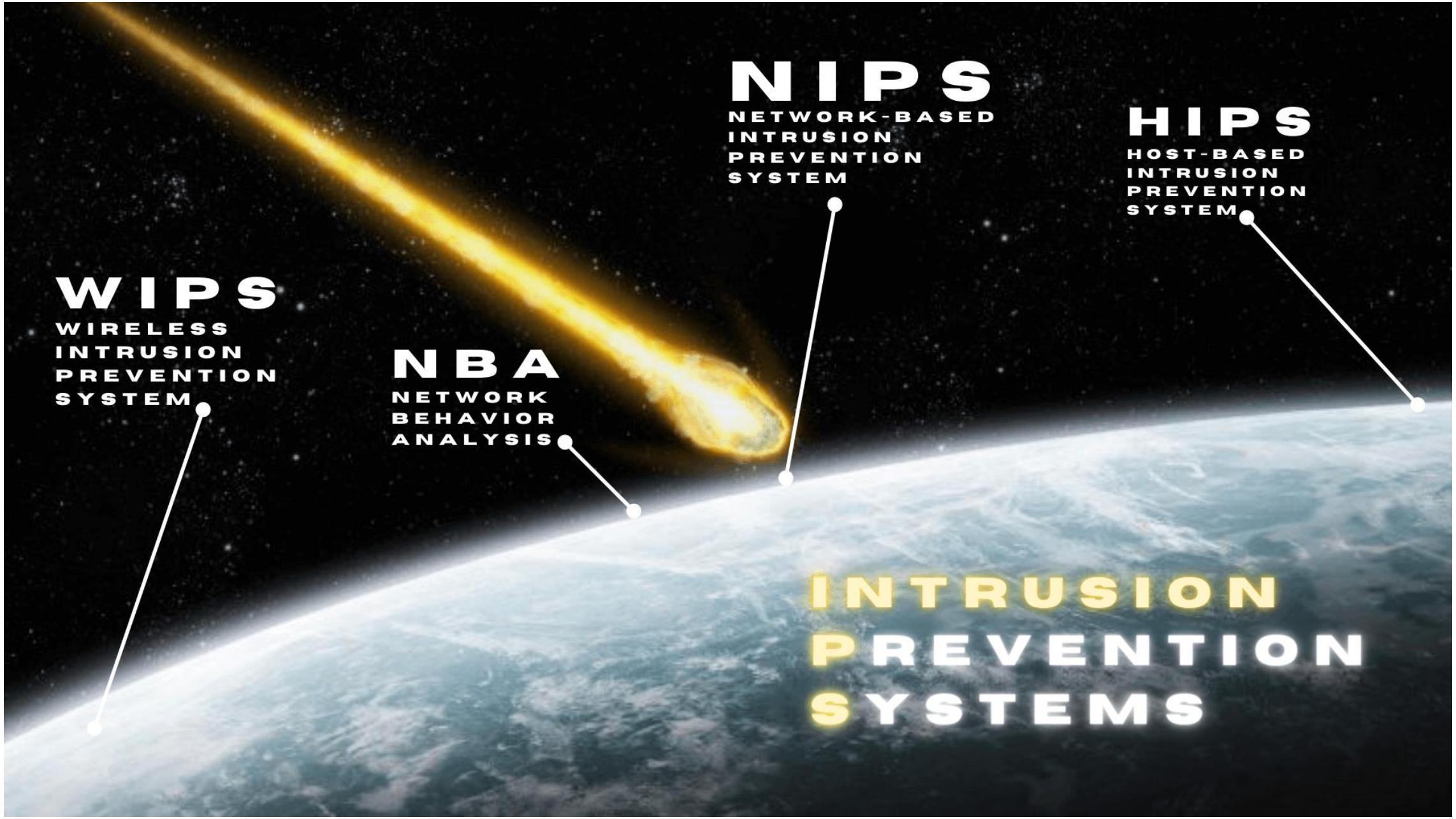
O NIPS apresenta a propriedade de efetuar *drop* na conexão, impedindo, dessa forma, que os pacotes cheguem ao seu destino, tal como os *firewalls* atuam.

Ele possui acesso direto ao sistema operacional da máquina e ao próprio kernel, podendo dessa forma controlar os acessos ao sistema de arquivos, configuração e registros do sistema.

Sistema de Prevenção de intrusão baseado em host (HIPS)

O principal do HIPS é que ele identifica comportamentos suspeitos no sistema operacional, ao invés de comparar assinaturas.

Além disso, o HIPS traz a possibilidade de que o tráfego de rede criptografado seja identificado após o processo de descriptografia do pacote, possibilitando a detecção do ataque antes cifrado, fato que não ocorre no uso do NIPS e NIDS.


NIPS
NETWORK-BASED
INTRUSION
PREVENTION
SYSTEM
HIPS
HOST-BASED
INTRUSION
PREVENTION
SYSTEM
WIPS
WIRELESS
INTRUSION
PREVENTION
SYSTEM
NBA
NETWORK
BEHAVIOR
ANALYSIS
INTRUSION
PREVENTION
SYSTEMS

IDS e IPS

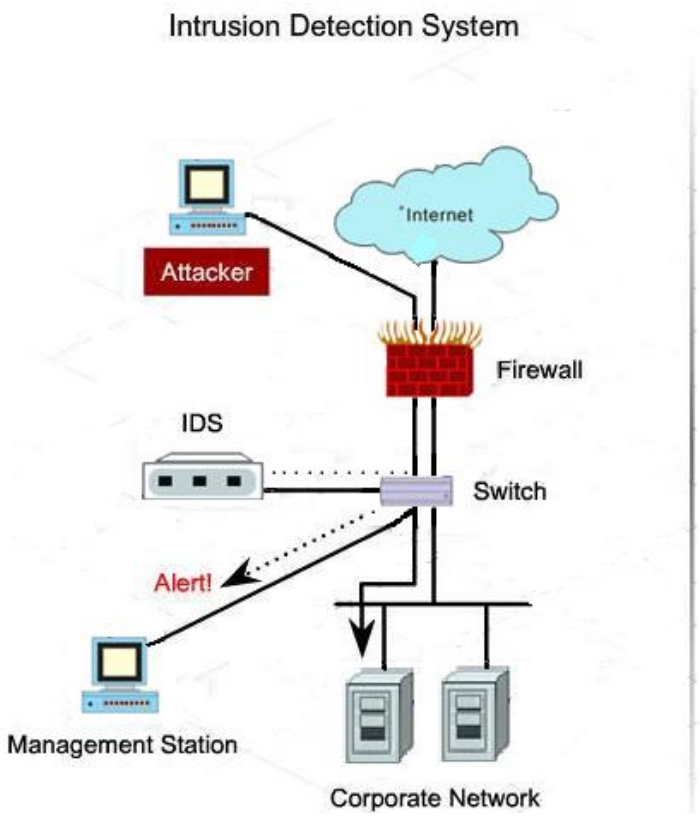
prevenção. Ambos IDS e IPS necessitam de uma
para realizarem a comparação com possíveis ata
No entanto, o IDS se restringe a detectar tentativ
administrador da rede. O IPS opera "*inline*" na re
bloquear as intrusões em tempo real.
Com respaldo na análise feita pelo IDS, o IPS repr
bloqueia o endereço IP do invasor, enquanto ele
que ele ocorra.

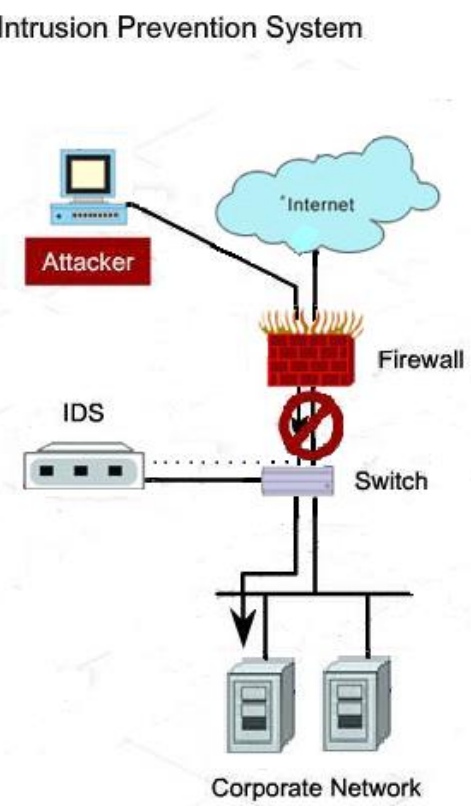
aturas conhecidas

-las e enviá-las ao
adicionais para

maticamente e
do o ataque, antes

IDS X IPS


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network

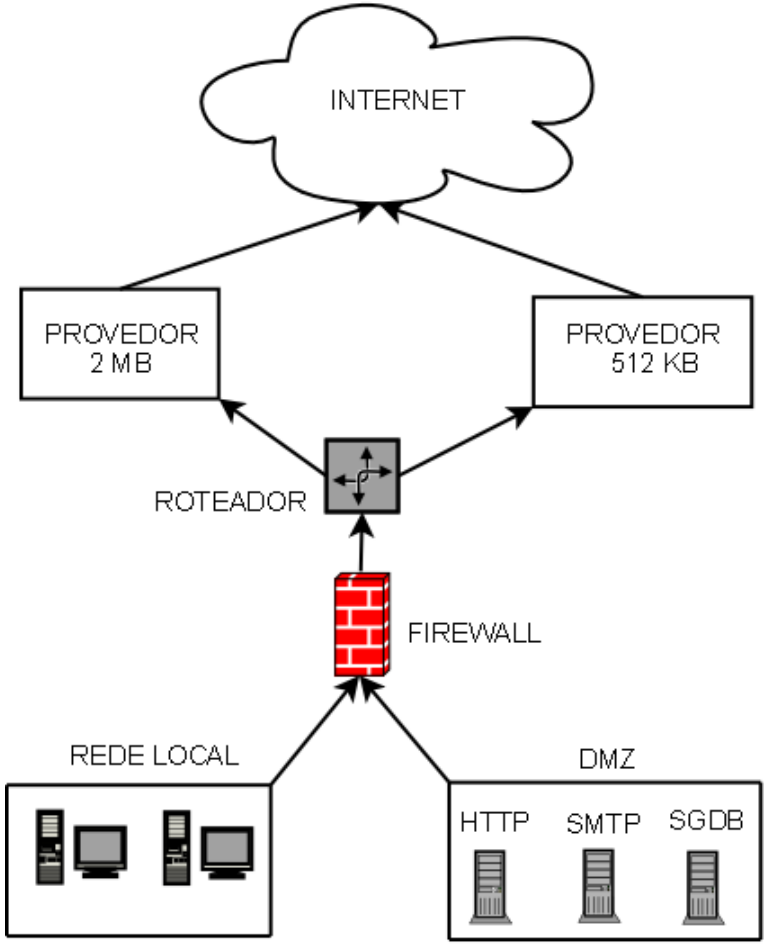

Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network


IDS
IPS

Zona Desmilitarizada - ZDM

Também conhecida como “DMZ” – Demilitarized Zone ou rede de perímetro.

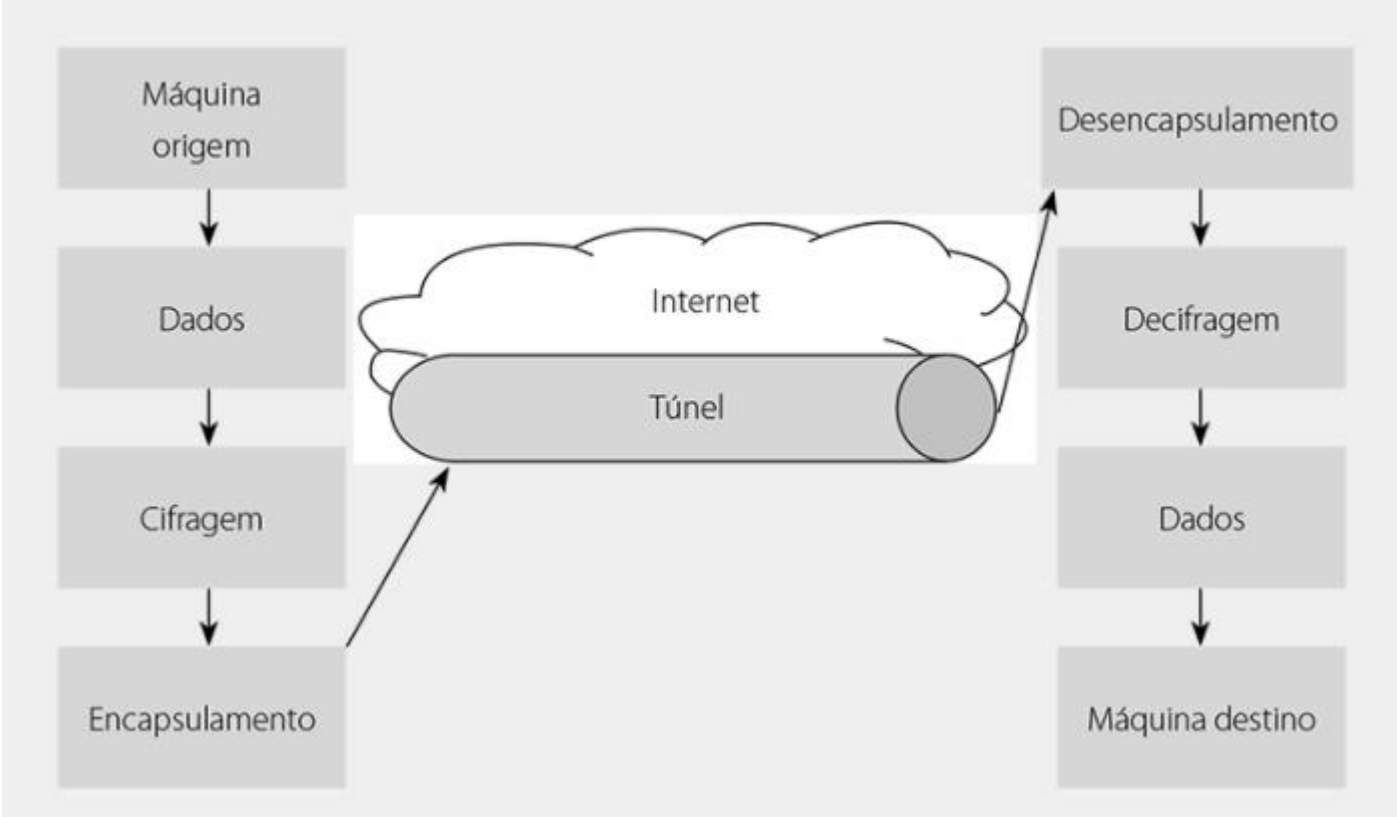
- sub-rede que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a internet;
- dispositivos situados nesta área, estão na zona desmilitarizada;
- Isola os serviços de acesso externo à rede local da organização, limitando o potencial dano em caso de comprometimento de algum desses serviços por um invasor.



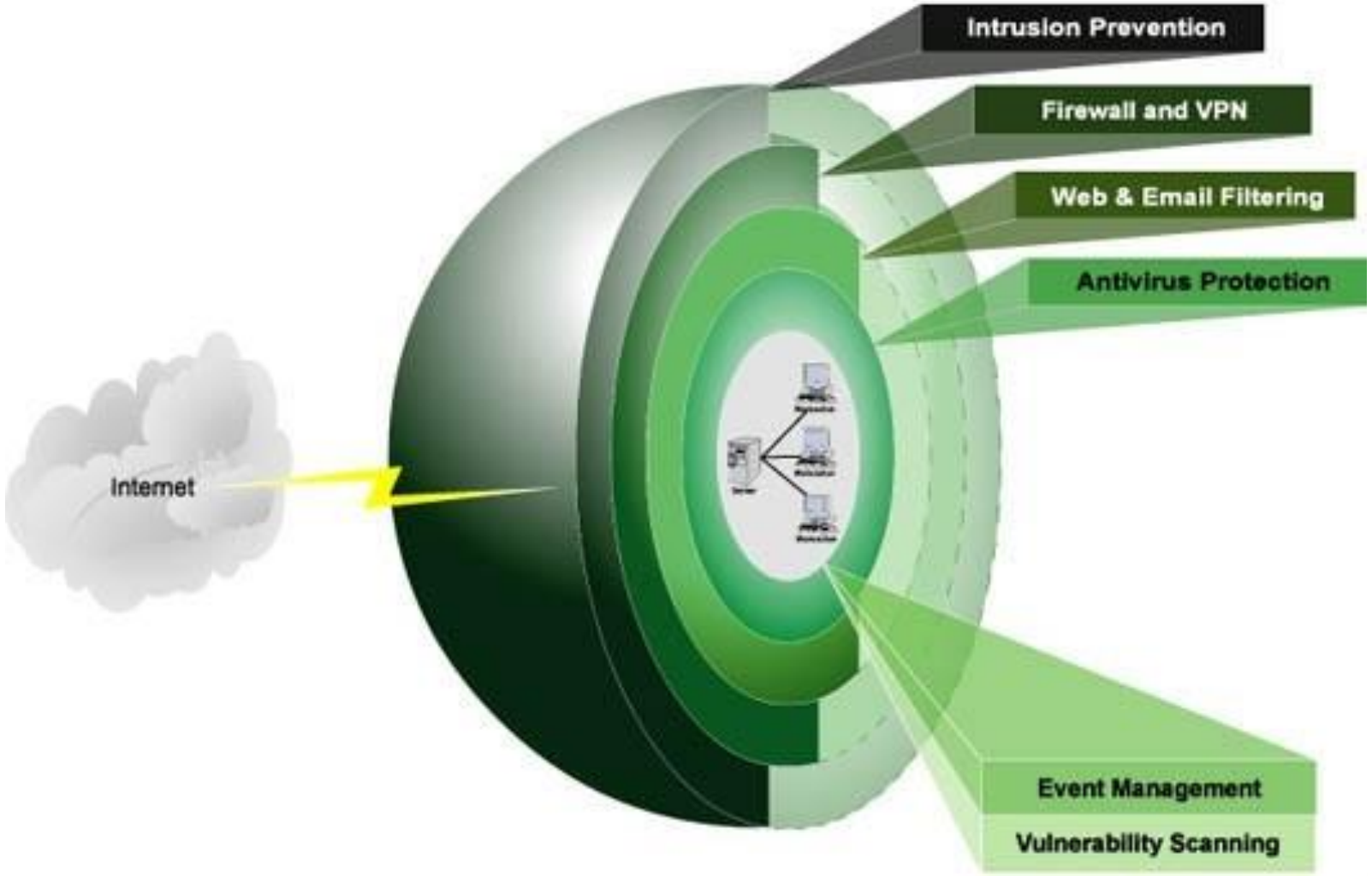
https://pt.wikipedia.org/wiki/DMZ_(computa%C3%A7%C3%A3o)

VPN – Virtual Private Network

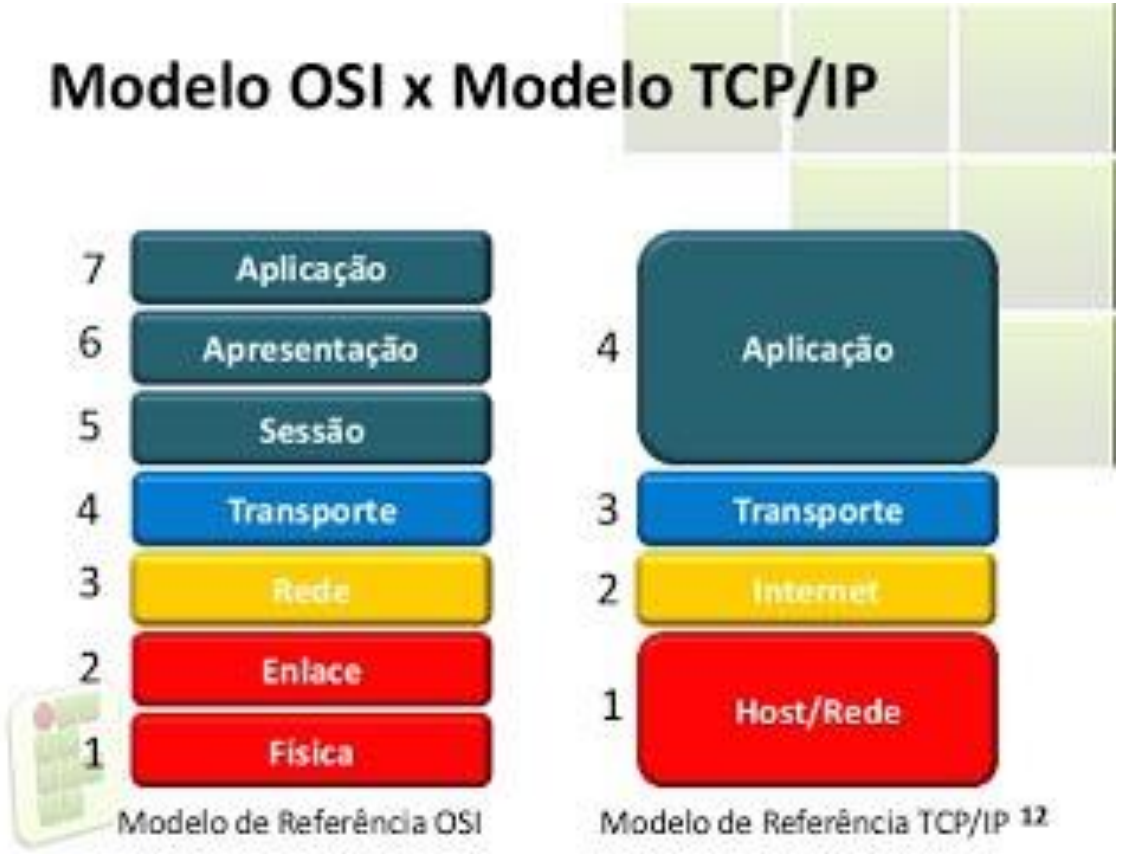
- Uso da Internet;
- Criptografia e processos de tunelamento;
- Túnel virtual entre máquinas de origem e destino.



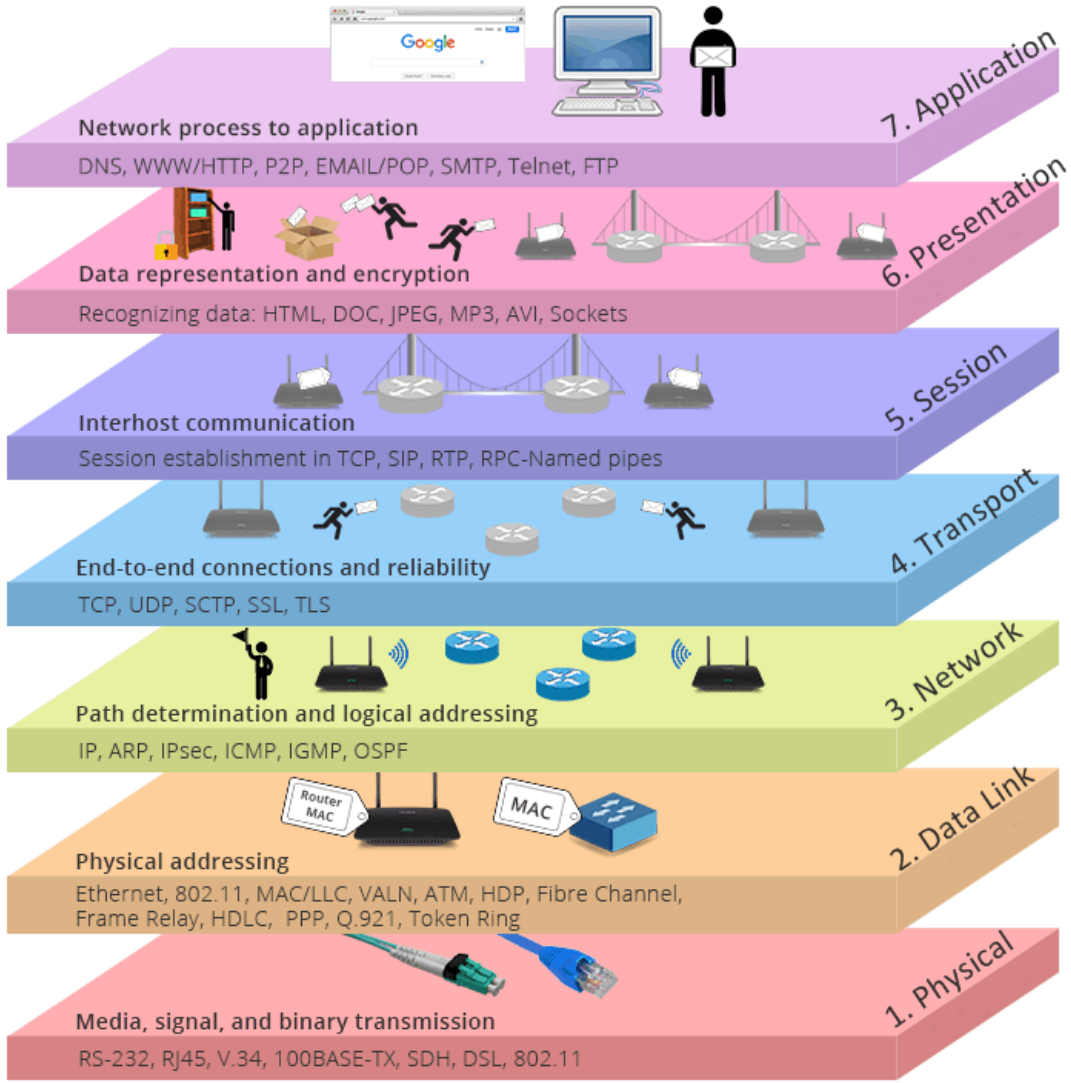
Proteção em Camadas



Modelo de referência



Modelo de referência ISO/OSI



Arquitetura OSI de Segurança

- A arquitetura OSI de segurança é baseada na *recomendação X.800** e se baseia na necessidade das organizações possuírem políticas de segurança e serviços que permitam avaliar tudo o que esteja relacionado com a segurança de suas informações. (*ITU-T)

- Descreve os recursos básicos que devem ser considerados quando você quer conectar um computador a outros, seja conectado à Internet ou a uma rede local, com segurança.

- Aborda três aspectos
  - Ataque à segurança (Passivo ou Ativo) – ação que compromete a segurança;
  - Serviço de segurança – utilizam um ou mais mecanismos p/ frustrar ataques;
  - Mecanismo de segurança – processo ou dispositivo (detectar/impedir/recuperar).

autenticidade e disponibilidade dos dados.

O que a X 800 considera um ataque à segurança, como eles são classificados, explique?

O que é x 800?

Tanto nas recomendações X. 800 da ITU-T, quanto na RFC 2828, os ataques à segurança são classificados como ataques passivos e ataques ativos. Um ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta seus recursos. Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação

RFC 2828 (Internet Security Glossary).(Adversário, ameaça, ataque, risco…

Padronização

- **National Institute of Standards and Technology (NIST):** federal dos EUA que lida com a ciência da medição, padrões e tecnologia relacionados ao uso do governo e à promoção de inovação no setor privado norte-americano. Apesar de seu escopo nacional, a Federal Information Processing Standards (FIPS) e a Special Publications (SP) do NIST têm um impacto mundial.
- **Internet Society (ISOC):** sociedade de membros profissionais com participação organizacional e individual no mundo inteiro. Ela oferece liderança no tratamento de questões que se referem ao futuro da Internet e é a organização pai para os grupos responsáveis por padrões de infraestrutura da Internet, incluindo a Internet Engineering Task Force (IETF) e o Internet Architecture Board (IAB). Essas organizações desenvolvem padrões da Internet e especificações relacionadas, todos publicados como Requests for Comments (RFCs).
- **ITU-T The International Telecommunication Union (ITU):** organização internacional dentro do Sistema das Nações Unidas em que os governos e o setor privado coordenam redes e serviços de telecomunicação global. O ITU Telecommunication Standardization Sector (ITU-T) é um dos três setores da ITU. A missão da ITU-T é a produção de padrões que abrangem todos os campos das telecomunicações. Os padrões ITU-T são chamados de Recomendações.
- **International Organization for Standardization (ISO)[1]:** federação mundial de agências de padrões nacionais para mais de 140 países, uma de cada país. ISO é uma organização não governamental, que promove o desenvolvimento da padronização e atividades relacionadas, com uma visão para facilitar a troca internacional de bens e serviços e desenvolver a cooperação nas esferas da atividade intelectual, científica, tecnológica e econômica. O trabalho da ISO resulta em acordos internacionais que são publicados como Padrões Internacionais.

Serviços de Segurança

- Dividido em 5 categorias e 14 serviços específicos

AUTENTICAÇÃO

A certeza de que a entidade se comunicando é aquela que ela afirma ser.

Autenticação de entidade pareada
Usada em associação com uma conexão lógica para fornecer confiança na identidade das entidades conectadas.

Autenticação da origem de dados
Em uma transferência sem conexão, oferece certeza de que a origem dos dados recebidos é conforme alegada.

CONTROLE DE ACESSO

A prevenção de uso não autorizado de um recurso (ou seja, esse serviço controla quem pode ter acesso a um recurso, sob que condições o acesso pode ocorrer e o que é permitido àqueles que acessam o recurso).

CONFIDENCIALIDADE DOS DADOS

A proteção dos dados contra divulgação não autorizada.

Confidencialidade da conexão
A proteção de todos os dados do usuário em uma conexão.

Confidencialidade sem conexão
A proteção de todos os dados do usuário em um único bloco de dados.

Confidencialidade com campo seletivo
A confidencialidade de campos selecionados dentro dos dados do usuário em uma conexão ou em um único bloco de dados.

Confidencialidade do fluxo de tráfego
A proteção das informações que poderiam ser derivadas dos fluxos de tráfego.

Serviços de Segurança

INTEGRIDADE DE DADOS

A certeza de que os dados recebidos são exatamente conforme enviados por uma entidade autorizada (ou seja, não contêm modificação, inserção, exclusão ou repasse).

Integridade da conexão com recuperação
Providencia a integridade de todos os dados do usuário em uma conexão e detecta qualquer modificação, inserção, exclusão ou repasse de quaisquer dados dentro de uma sequência inteira, com tentativa de recuperação.

Integridade da conexão sem recuperação
Como acima, mas oferece apenas detecção sem tentativa de recuperação.

Integridade da conexão com campo seletivo
Providencia a integridade de campos selecionados nos dados do usuário de um bloco de dados transferido por uma conexão e determina se os campos selecionados foram modificados, inseridos, excluídos ou repassados.

Integridade sem conexão
Providencia a integridade de um único bloco de dados sem conexão e pode tomar a forma de detecção da modificação de dados. Além disso, pode haver uma forma limitada de detecção de repasse.

Integridade sem conexão com campo seletivo
Providencia a integridade de campos selecionados dentro de um único bloco de dados sem conexão; determina se os campos selecionados foram modificados.

IRRETRATABILIDADE

Oferece proteção contra negação, por parte de uma das entidades envolvidas em uma comunicação, de ter participado de toda ou parte dela.

Irretratabilidade, Origem
Prova de que a mensagem foi enviada pela parte especificada.

Irretratabilidade, Destino
Prova de que a mensagem foi recebida pela parte especificada.

Mecanismos de Segurança Específicos

MECANISMOS DE SEGURANÇA ESPECÍFICOS

Podem ser incorporados à camada de protocolo apropriada a fim de oferecer alguns dos serviços de segurança OSI.

Codificação
O uso de algoritmos matemáticos para transformar os dados para um formato que não seja prontamente inteligível. A transformação e subsequente recuperação dos dados depende de um algoritmo e zero ou mais chaves de encriptação.

Assinatura digital
Dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário dela prove sua origem e integridade e a proteja contra falsificação (por exemplo, pelo destinatário).

Controle de acesso
Uma série de mecanismos que impõem direitos de acesso aos recursos.

Integridade de dados
Uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.

Troca de autenticação
Um mecanismo intencionado a garantir a identidade de uma entidade por meio da troca de informações.

Preenchimento de tráfego
A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

Controle de roteamento
Permite a seleção de determinadas rotas fisicamente seguras para certos dados e mudanças de roteamento, sobretudo quando uma brecha de segurança é suspeitada.

Notarização
O uso de um terceiro confiável para garantir certas propriedades de uma troca de dados.

Mecanismos de Segurança Difusos

MECANISMOS DE SEGURANÇA DIFUSOS

Mecanismos que não são específicos a qualquer serviço de servidor OSI ou camada de protocolo específica.

Funcionalidade confiada
Aquilo que é percebido como sendo correto com relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).

Rótulo de segurança
A marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.

Detecção de evento
Detecção de eventos relevantes à segurança.

Trilha de auditoria de segurança
Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e das atividades do sistema.

Recuperação de segurança
Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

Bibliografia

- Criptografia e Segurança de Redes – Princípios e Práticas, 6ª edição - William Stalings

- Fundamentos em Segurança da Informação
Michele da Costa Galvão

- Sistemas de Segurança da Informação na era do conhecimento
Armando Kolbe Júnior

- https://pt.wikipedia.org/

- https://www.antivirusguide.com/best-firewall/

- https://northernblock.io/

OBRIGADO!