1.Zero Trust

É uma abordagem que busca redefinir a maneira como as redes e os sistemas são protegidos. Tradicionalmente, os modelos de segurança de perímetro confiavam em uma defesa baseada na ideia de "confiança implícita". Ou seja, uma vez que um dispositivo ou usuário estivesse dentro do perímetro da rede, eles seriam considerados confiáveis e teriam acesso a recursos e dados.

Zero Trust adota uma mentalidade oposta, onde nenhum dispositivo ou usuário é confiável por padrão. Em vez disso, a segurança é baseada na autenticação, na autorização e na verificação contínua em todos os momentos. O princípio fundamental é que cada solicitação de acesso, seja de um dispositivo ou usuário interno ou externo, deve ser verificada e autenticada independentemente de estar dentro ou fora do perímetro da rede. Existem planos de operação que dividem a rede em planos funcionais.

2.Plano de dados

Responsável por *frames*, pacotes e dados de rede, além do processamento, encaminhamento, *trunking*, criptografia e rede NAT

2.1 Implicit trust zone

É uma área ou componente de um sistema de segurança onde a confiança é assumida sem a necessidade de uma verificação explícita. Em termos simples, são partes de um sistema que são consideradas seguras sem serem constantemente monitoradas ou auditadas. Esse conceito é frequentemente aplicado em arquitetura de redes ou sistemas, onde certas áreas, como a rede interna de uma organização, são consideradas "confiáveis" sem que cada interação ou transação seja verificada, já que se presume que as ameaças externas não têm acesso a essa zona.

2.2 Subject/System

Refere-se à identificação e controle de quem ou o quê está acessando recursos na rede.

- **Subject (Sujeito)**: Um usuário, serviço ou identidade que faz uma solicitação de acesso. Pode ser um humano (usuário final, administrador) ou uma identidade de máquina (como um serviço ou aplicação).
- **System (Sistema)**: O recurso ou ambiente que está sendo acessado, como um servidor, banco de dados ou serviço na nuvem.

No Zero Trust, cada requisição de acesso deve ser autenticada e autorizada individualmente, levando em conta identidade, contexto e postura de segurança. Isso reduz o risco de movimentação lateral e acessos indevidos dentro do ambiente.

2.3 Policy Enforcement Point (PEP)

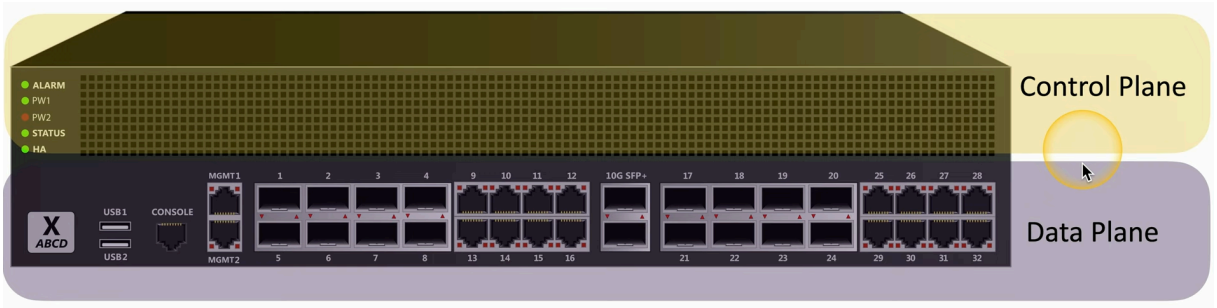
O **Policy Enforcement Point (PEP)** é um componente essencial na arquitetura **Zero Trust**, responsável por **interceptar e aplicar as políticas de acesso** definidas pelo sistema de segurança.

- **Intermedia o acesso** entre o usuário (ou sistema) e o recurso solicitado.
- **Avalia** se a solicitação está em conformidade com as regras de segurança.
- **Consulta o Policy Decision Point (PDP)** para determinar se a solicitação deve ser **permitida ou bloqueada**.
- **Aplica a decisão** do PDP, garantindo que apenas acessos autorizados sejam concedidos.

O PEP pode estar presente em firewalls, proxies, gateways, agentes em endpoints e outros mecanismos de controle, assegurando que cada acesso seja verificado antes de ser concedido.

3.Plano de controle

Responsável pelas ações feitas do plano de dados, definindo regras e políticas de segurança. Determina como os pacotes serão encaminhados através da rede configurando e gerenciando tabelas de roteamento, tabelas de sessão e tabelas NAT.

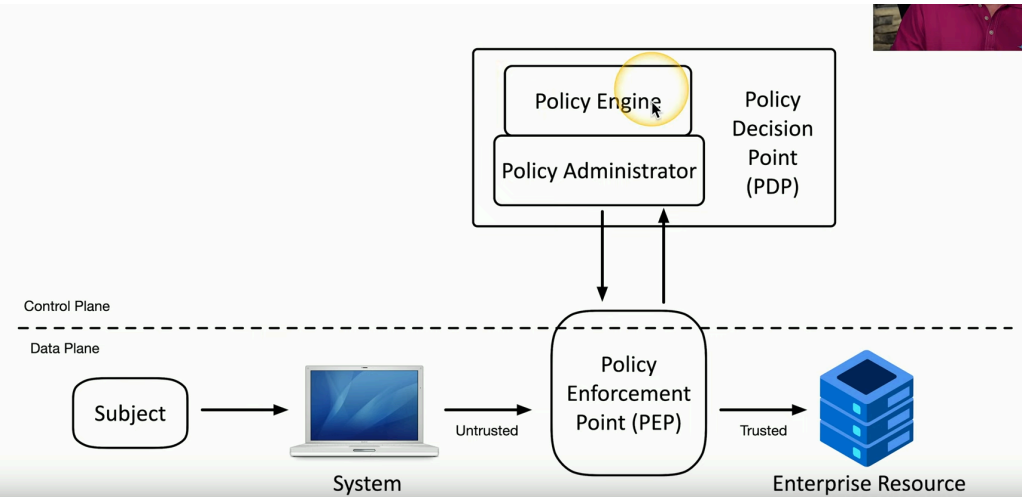


3.1 Identidade adaptativa

<u>Identidade adaptativa considera a origem e quem está requisitando dados</u>. Existem diversos indicadores de risco como: relacionamento com a organização, localização física, tipo de conexão, endereço IP e outros. Através destes dados, é possível criar uma autenticação mais forte e robusta, se necessário.

Segurança vai além de relações de 1:1. A categorização ampla provê uma fundamentação da relação segura. De onde você está vindo? É de uma rede confiável ou não? Redes externas e internas. Qual VPN?

Zero trust através dos planos na imagem abaixo



3.2 Policy-driven Access Control

Policy-Driven Access Control (PDAC) é um modelo de controle de acesso baseado em políticas predefinidas, que determinam quem pode acessar quais recursos, em quais condições e com quais permissões. Diferente dos modelos tradicionais baseados apenas em regras estáticas, o PDAC avalia o contexto e permite uma abordagem mais dinâmica e adaptável à segurança.

Baseado em Políticas – O acesso é concedido ou negado com base em um conjunto de regras definidas por políticas de segurança, em vez de apenas listas de controle de acesso (ACLs) fixas.

Avaliação Contínua – O acesso pode ser revisado em tempo real, considerando mudanças contextuais, como localização do usuário, dispositivo utilizado, horário e nível de risco.

Integração com Modelos de Controle de Acesso – O PDAC pode ser implementado usando abordagens como:

- **ABAC (Attribute-Based Access Control)**: Considera atributos do usuário, recurso e ambiente.
- **RBAC (Role-Based Access Control) Dinâmico**: Permissões baseadas em funções, mas com ajustes dinâmicos baseados em contexto.

Alinhamento com Zero Trust – Como não há confiança implícita, cada solicitação de acesso passa por uma verificação rigorosa e contínua.

3.3 Policy Administrator

O **Policy Administrator (PA)** é um componente da arquitetura **Zero Trust** responsável por **gerenciar e distribuir políticas de acesso** dentro do sistema de controle de acesso baseado em políticas (**Policy-Driven Access Control – PDAC**).

- **Recebe a decisão do Policy Decision Point (PDP)** – Após o PDP avaliar se um acesso deve ser permitido ou negado, o PA transforma essa decisão em uma ação prática.
- **Distribui a decisão ao Policy Enforcement Point (PEP)** – O PEP é o componente que efetivamente aplica a política no sistema, bloqueando ou permitindo o acesso.
- **Garante a consistência e atualização das políticas** – O PA pode modificar, atualizar e revogar políticas dinamicamente para atender às mudanças na segurança.

O Policy Administrator atua como intermediário entre **a lógica de decisão (PDP)** e **a aplicação das políticas (PEP)**, garantindo que os acessos sejam controlados de acordo com as regras organizacionais.

3.4 Policy Engine

O **Policy Engine (PE)** é o componente da arquitetura **Zero Trust** responsável por **avaliar e decidir** se uma solicitação de acesso deve ser permitida ou negada com base em políticas de segurança definidas.

Analisa regras e políticas de acesso – Considera identidades, contexto, riscos e conformidade para tomar decisões.

Trabalha em conjunto com o Policy Decision Point (PDP) – Atua como o mecanismo central de decisão dentro do PDP.

Consulta fontes externas – Pode verificar logs, inteligência de ameaças e dados de conformidade antes de emitir um veredito.

Fornece decisões dinâmicas – Avalia cada solicitação em tempo real, garantindo que acessos sejam revisados continuamente.