
TIC
AULA 15
PROF: ROBERTO

O QUE VAMOS VER NESSA AULA

- NAT:
  - Tipos de NAT:
    - Estático;
    - Dinâmico;
    - PAT.
  - Casos de uso;
- Firewall
  - Conceitos;
  - Tipos.
- Firewall de Zona:
  - Simulando

1.

NAT

Network Address Translation

INTRODUÇÃO AO NAT E CONCEITOS BÁSICOS

O que é NAT (Network Address Translation):

- NAT é uma técnica utilizada para permitir que múltiplos dispositivos dentro de uma rede privada utilizem um ou mais endereços IP públicos para se comunicar com outras redes, como a internet.
- Foi criado para resolver o problema da escassez de endereços IPv4, ao permitir que redes internas utilizem endereços privados que não são roteados pela internet.

Por que o NAT é importante:

- **Segurança:** NAT também esconde os endereços IP privados, proporcionando uma camada extra de segurança, pois os dispositivos da rede externa (como a internet) não conseguem acessar diretamente os dispositivos internos.
- **Eficiência no uso de IPs:** NAT permite que várias máquinas compartilhem um único endereço IP público, economizando endereços IPv4 públicos.

ENDEREÇOS IP PÚBLICOS E PRIVADOS

- **Endereços IP Públicos:** Um endereço único e globalmente roteável utilizado para identificar dispositivos na internet.
- **Atribuição de IPs Públicos:** Controlada pela IANA (Internet Assigned Numbers Authority) e distribuída por organizações regionais.
- **Endereços IP Privados:** Usado em redes internas que não são roteadas diretamente pela internet.
  - Faixas de IP Privado: Determinadas pela RFC 1918:
    - Classe A: 10.0.0.0 a 10.255.255.255
    - Classe B: 172.16.0.0 a 172.31.255.255
    - Classe C: 192.168.0.0 a 192.168.255.255
  - Dispositivos que usam endereços privados precisam de um gateway com NAT para acessar a internet.

TIPOS DE NAT

NAT Estático (1 para 1):

- **Definição:**
  - Cada endereço IP privado é mapeado para um endereço IP público fixo.

- **Casos de uso:** Quando você quer que um servidor interno seja acessível externamente, como um servidor web ou servidor de e-mail.

- **Exemplo:**
  - 192.168.1.10 (servidor interno) é mapeado para 200.1.1.10 (endereço público). Toda solicitação ao 200.1.1.10 será encaminhada para o servidor 192.168.1.10.

TIPOS DE NAT

NAT Dinâmico (Conjunto de endereços públicos):

- **Definição:**
  - Um conjunto de endereços IP privados é mapeado dinamicamente para um conjunto de endereços IP públicos disponíveis.
- **Casos de uso:** Quando há um número limitado de IPs públicos e não é necessário que cada dispositivo tenha um IP público fixo.
- **Exemplo:**
  - Uma rede interna com endereços 192.168.1.0/24 utiliza um pool de endereços IP públicos, como 200.1.1.10 a 200.1.1.20, e cada dispositivo usa um IP público quando necessário.

TIPOS DE NAT

PAT (Port Address Translation) ou NAT Sobrecarga (Múltiplos dispositivos para um IP público):

- **Definição:**
  - Vários endereços IP privados compartilham um único endereço IP público, diferenciando-se pelas portas TCP/UDP.
- **Casos de uso:** Cenário mais comum em redes domésticas e pequenas empresas, onde apenas um endereço IP público é usado para todos os dispositivos internos.
- **Exemplo:**
  - 192.168.1.2, 192.168.1.3, e 192.168.1.4 compartilham o endereço IP público 200.1.1.10. Cada dispositivo usa uma porta diferente para as conexões.

CASOS DE USO

- **Rede Doméstica:** Em casa, todos os dispositivos (PCs, smartphones, TVs) usam endereços IP privados, como 192.168.0.x. O roteador, que está conectado à internet, usa NAT para permitir que todos esses dispositivos compartilhem o mesmo IP público e acessem a internet.

- **Rede Corporativa:** Em uma empresa, vários departamentos estão em redes diferentes, todas utilizando endereços IP privados. O gateway NAT da empresa permite que os dispositivos dessas redes acessem a internet usando um conjunto de IPs públicos.

- **Data Centers e Servidores Públicos:** Um servidor em um data center usa NAT Estático para garantir que o mesmo endereço IP público seja sempre mapeado para ele, permitindo que clientes externos se conectem ao servidor via internet.

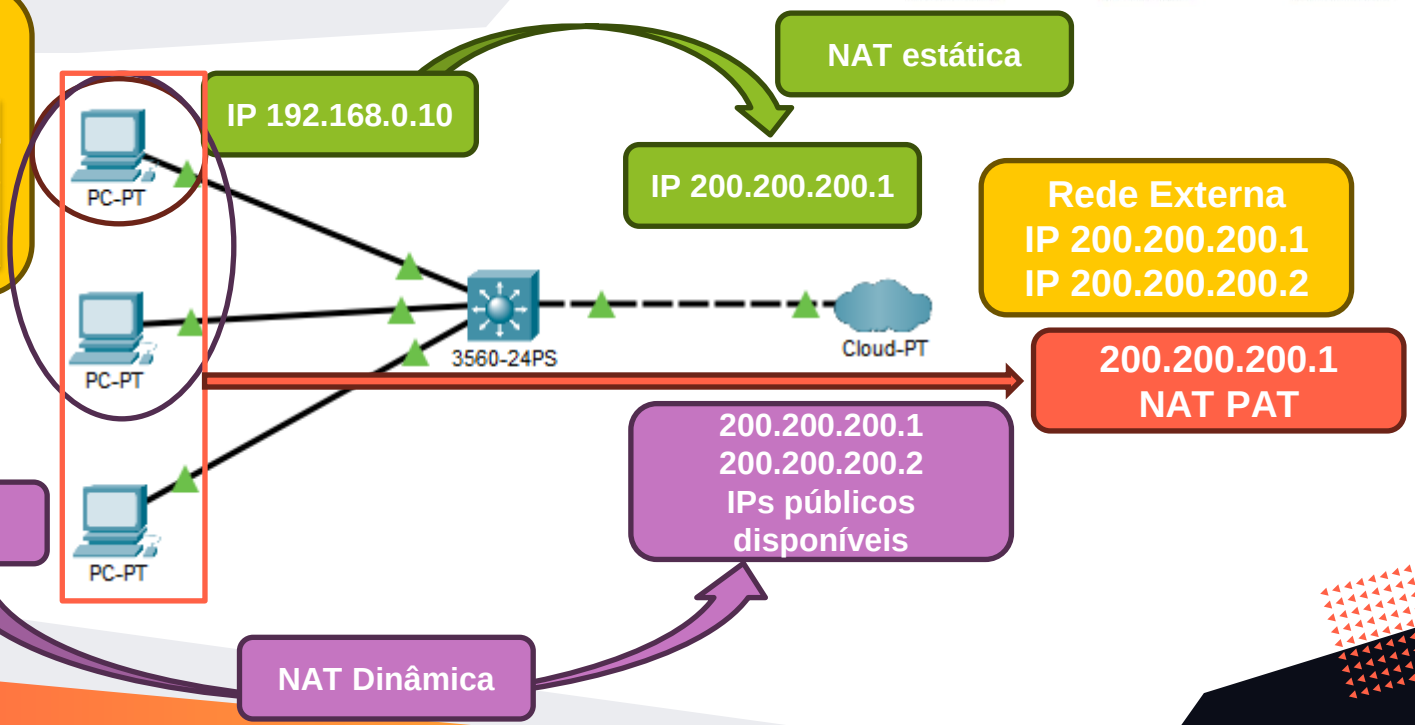
- **Segurança em Redes Corporativas:** Algumas empresas utilizam NAT como uma camada de segurança adicional, ao ocultar a rede interna e filtrar acessos externos via firewall.

NAT - TRADUÇÃO DE ENDEREÇOS DE REDE

É feita uma tabela para a tradução NAT

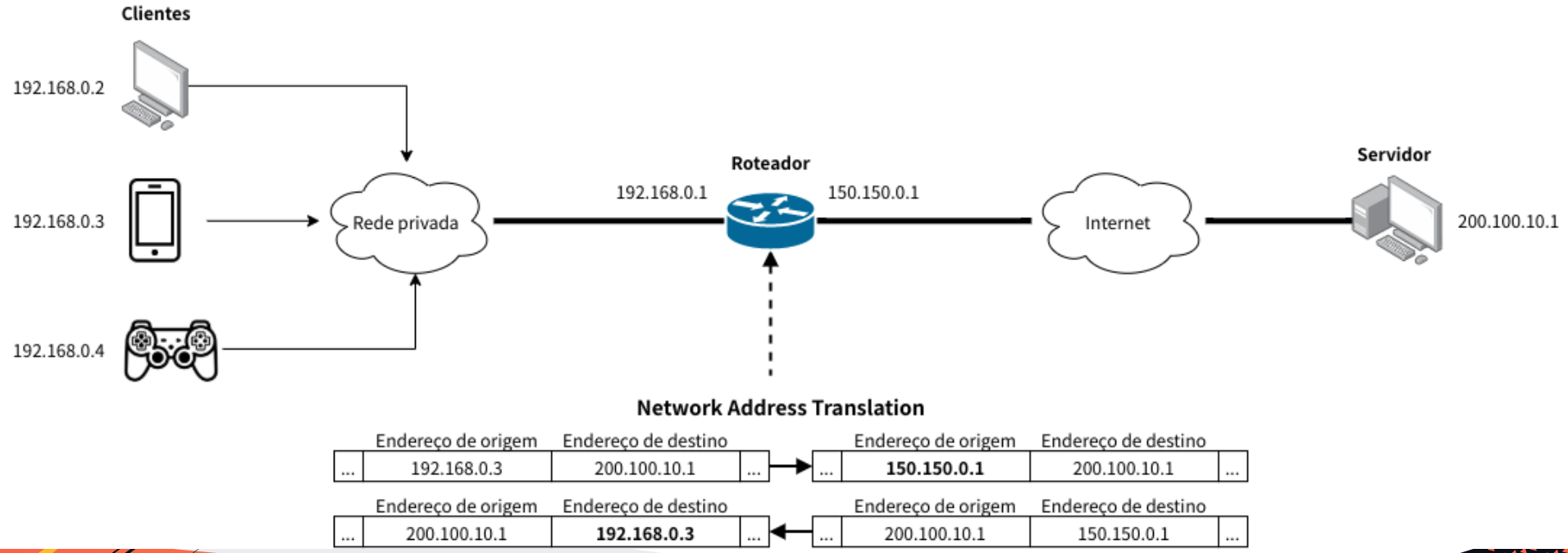
IP Privado	IP Público
192.168.0.10	200.200.200.1
192.168.0.11	200.200.200.1:5001(PAT)
192.168.0.12	200.200.200.1 ou 2

Rede interna
IP 192.168.0.0/24



NAT permite a comunicação entre redes internas e externas ao realizar a tradução de endereços IP de forma eficiente.

NAT



Network Address Translation

	Endereço de origem	Endereço de destino			Endereço de origem	Endereço de destino	
...	192.168.0.3	200.100.10.1	...	...	**150.150.0.1**	200.100.10.1	...

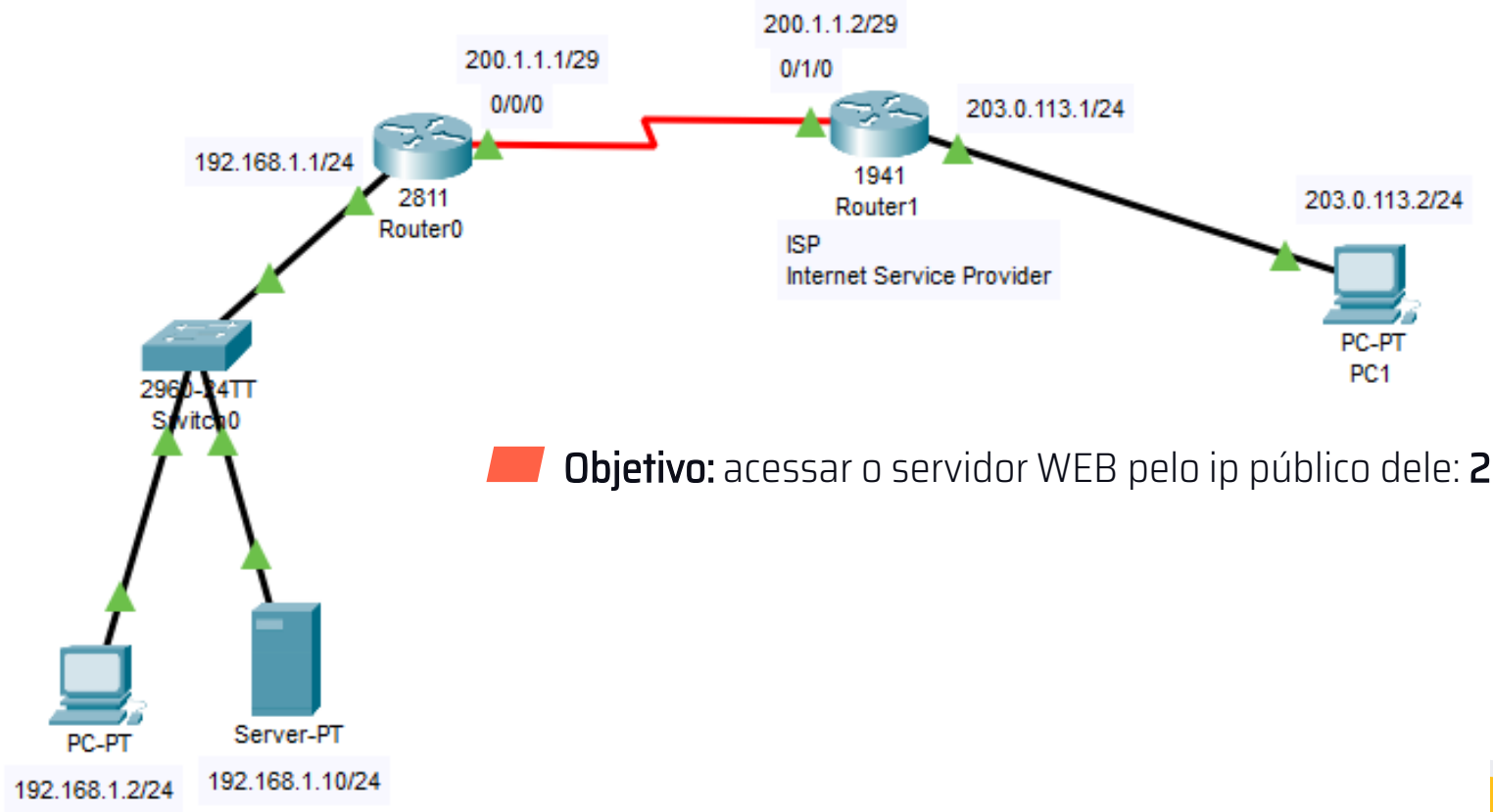
	Endereço de origem	Endereço de destino			Endereço de origem	Endereço de destino	
...	200.100.10.1	**192.168.0.3**	...	...	200.100.10.1	150.150.0.1	...

2.

SIMULANDO

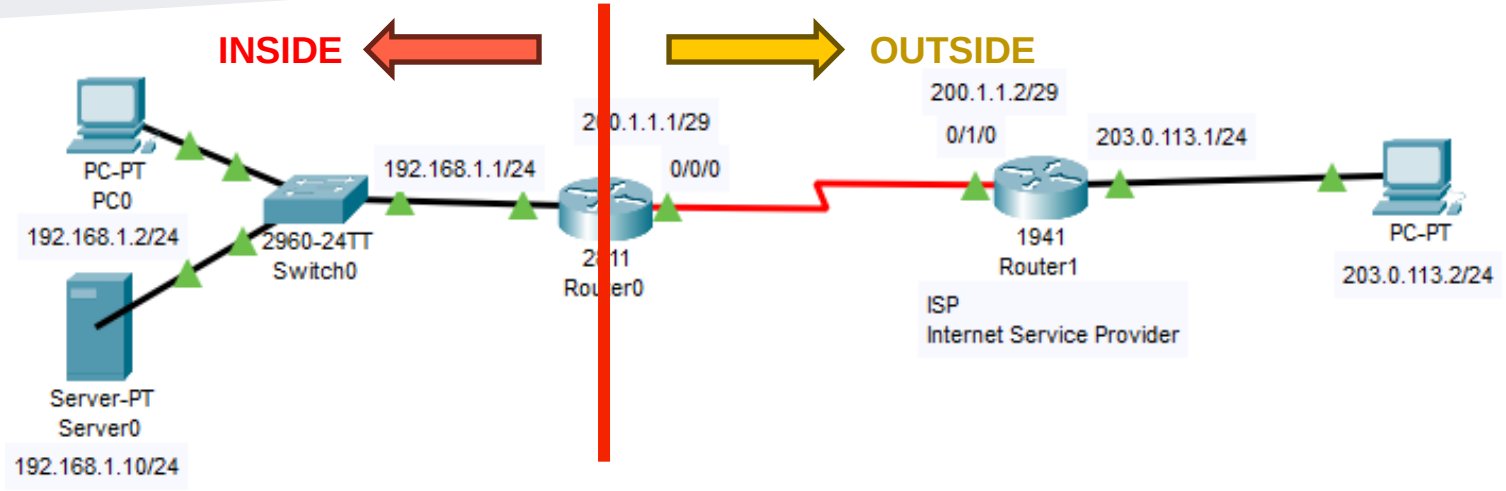
Network Address Translation

NAT ESTÁTICO - EXEMPLO



Objetivo: acessar o servidor WEB pelo ip público dele: **200.1.1.4**

NAT ESTÁTICO – EXEMPLO – INSIDE OUTSIDE

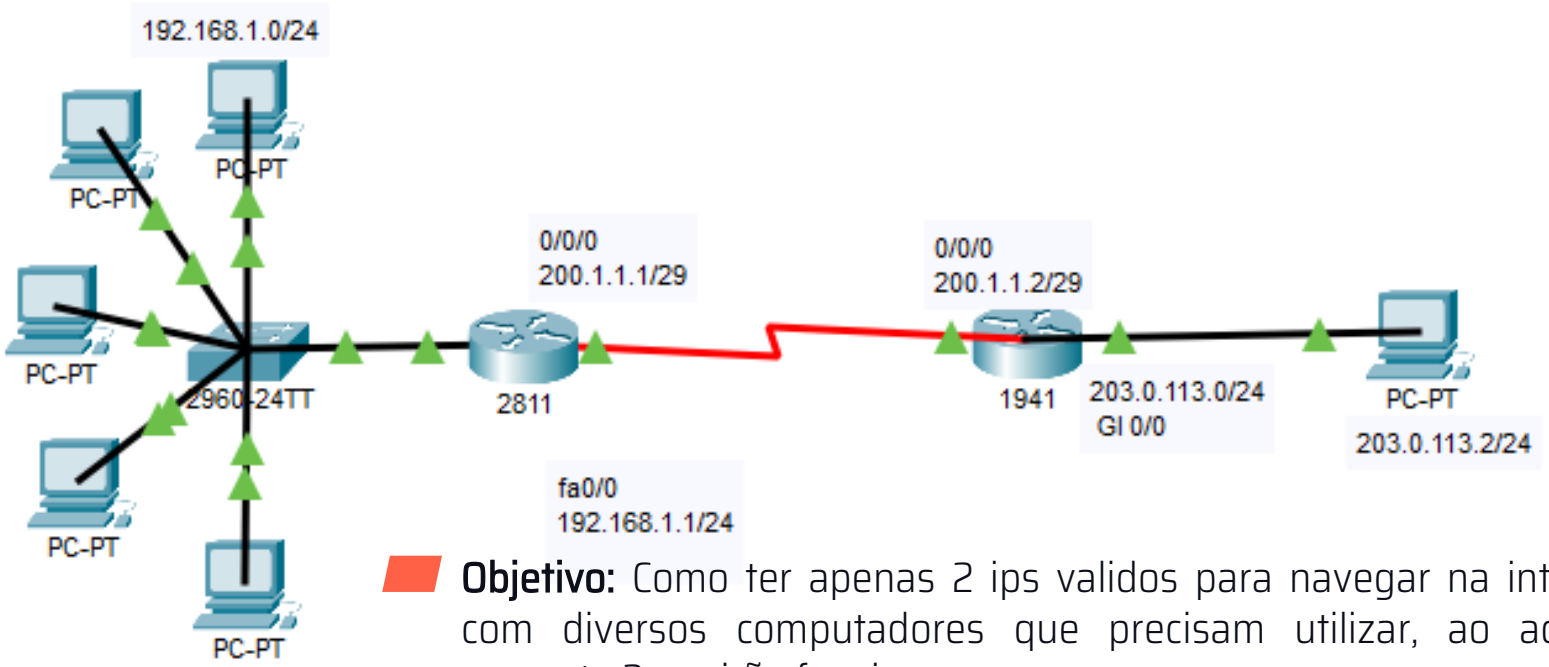


NAT ESTÁTICO - EXEMPLO

No roteador da Rede interna:

- interface fastEthernet 0/0
  - ip nat inside
- interface serial 0/0/0
  - Ip nat out
- ip nat inside source static 192.168.1.10 200.1.1.4
- Show ip nat translations
- Show ip nat statistics

NAT DINÂMICO - EXEMPLO



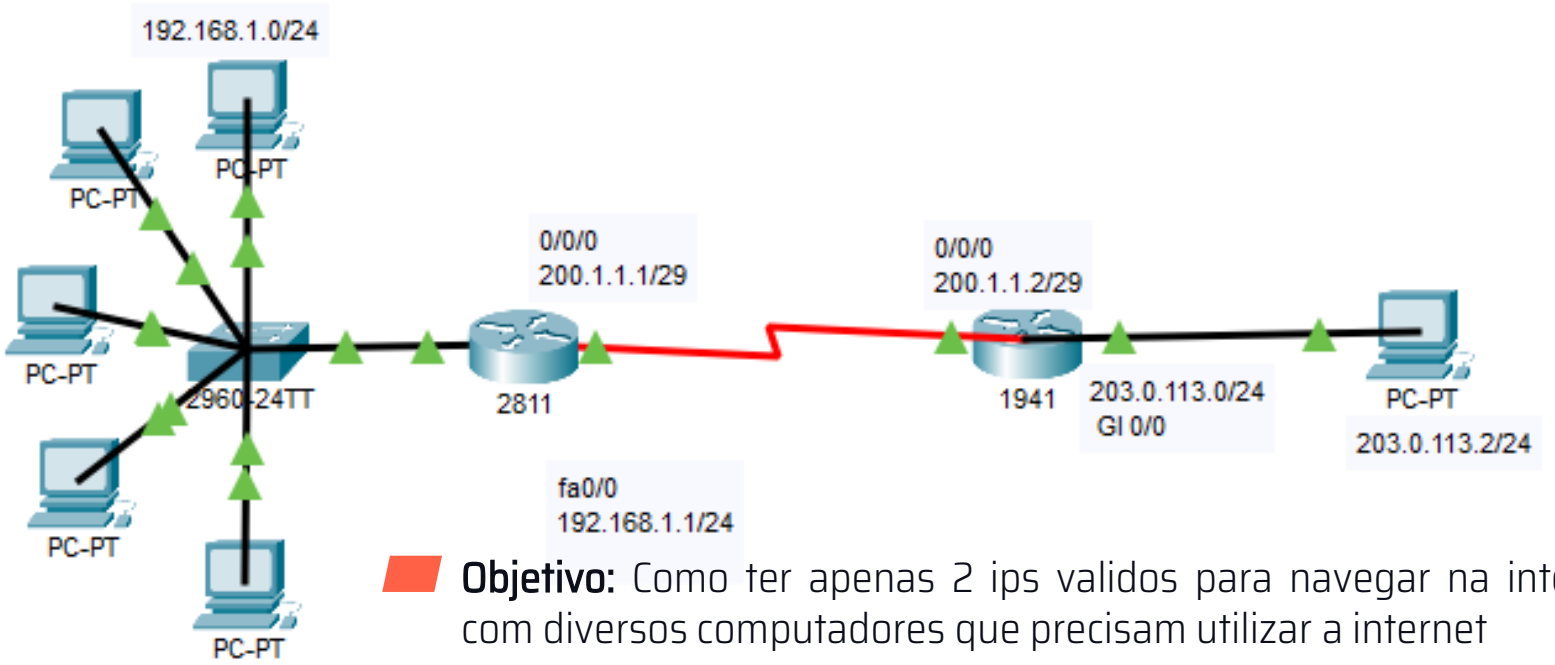
Objetivo: Como ter apenas 2 ips validos para navegar na internet, com diversos computadores que precisam utilizar, ao acessar somente 2 pcs irão funcionar

NAT DINÂMICO - EXEMPLO

- No roteador da Rede interna:
  - interface fastEthernet 0/0
    - ip nat inside
  - interface serial 0/0/0
    - Ip nat out
  - access-list 1 permit 192.168.1.0 0.0.0.255
  - ip nat pool teste 200.1.1.1 200.1.1.2 netmask 255.255.255.248
  - ip nat inside source list 1 pool teste
  - Show ip nat translations
  - Show ip nat statistics

- Caso tenhamos problemas temos comandos para ajudar:
  - **clear ip nat translation ***
  - **no ip nat inside source list 1 pool teste**

NAT DINÂMICO COM PAT- EXEMPLO



Objetivo: Como ter apenas 2 ips validos para navegar na internet, com diversos computadores que precisam utilizar a internet

NAT DINÂMICO - EXEMPLO

- No roteador da Rede interna:
  - interface fastEthernet 0/0
    - ip nat inside
  - interface serial 0/0/0
    - Ip nat out
  - access-list 1 permit 192.168.1.0 0.0.0.255
  - ip nat pool teste 200.1.1.1 200.1.1.2 netmask 255.255.255.248
  - ip nat inside source list 1 pool teste overload
  - Show ip nat translations
  - Show ip nat statistics

- Caso tenhamos problemas temos comandos para ajudar:
  - **clear ip nat translation ***
  - **no ip nat inside source list 1 pool teste**

2.

FIREWALL

conceitos

FIREWALL

- **Definição:** Um firewall é um dispositivo ou software de segurança que monitora e controla o tráfego de rede baseado em regras de segurança pré-definidas. Ele atua como uma barreira entre redes confiáveis (como a rede interna) e redes não confiáveis (como a internet).

- **Função Principal:** Proteger a rede interna contra ataques e acessos não autorizados, permitindo ou bloqueando o tráfego com base em regras de filtragem.

TIPOS DE FIREWALLS

Packet-Filtering Firewall (Filtro de Pacotes)

- **Como funciona:** Analisa cada pacote de dados individualmente, decidindo se permite ou bloqueia o pacote com base em regras predefinidas (por exemplo, IP de origem, IP de destino, porta e protocolo).
- **Vantagens:** Simples e eficiente para bloquear ou permitir tráfego básico.
- **Desvantagens:** Não monitora o estado da conexão e não oferece proteção contra ataques mais complexos, como ataques baseados em aplicações.

Stateful Inspection Firewall (Inspeção de Estado)

- **Como funciona:** Mantém o estado de cada conexão, permitindo ou bloqueando pacotes com base no estado da conexão (se é uma nova conexão, uma resposta ou parte de uma conexão já existente).
- **Vantagens:** Oferece maior controle, permitindo filtrar com base no contexto da conexão (por exemplo, bloqueia pacotes que não fazem parte de uma conexão estabelecida).
- **Desvantagens: Mais complexo e consome mais recursos.**

TIPOS DE FIREWALLS

Proxy Firewall

- **Como funciona:** Atua como intermediário entre o cliente e o servidor. O firewall proxy intercepta todas as comunicações e as retransmite, aplicando suas próprias regras de segurança.
- **Vantagens:** Esconde a identidade e o endereço IP dos clientes internos, oferecendo mais segurança e controle sobre o tráfego.
- **Desvantagens:** Introduz latência nas conexões, já que cada comunicação passa pelo firewall proxy.

Next-Generation Firewall (NGFW)

- **Como funciona:** Integra tecnologias avançadas, como inspeção profunda de pacotes, prevenção de intrusões (IPS), filtragem de aplicativos, e controle de tráfego com base no comportamento e nas identidades dos usuários.
- **Vantagens:** Oferece segurança mais completa, detectando e bloqueando ameaças avançadas.
- **Desvantagens:** Mais caro e complexo de implementar e gerenciar.

FIREWALLS BASEADOS EM HARDWARE VS. SOFTWARE

Firewall de Hardware

- **Onde é utilizado:** Implementado como um dispositivo dedicado, frequentemente posicionado entre a rede interna e a internet.
- **Vantagens:** Maior desempenho e pode proteger uma rede inteira.
- **Desvantagens:** Mais caro e requer mais conhecimento técnico para ser configurado e gerenciado.

Firewall de Software

- **Onde é utilizado:** Instalado em dispositivos individuais (como PCs e servidores) para proteger cada dispositivo.
- **Vantagens:** Mais acessível e fácil de instalar.
- **Desvantagens:** Só protege o dispositivo em que está instalado e consome recursos do sistema.

FIREWALLS BASEADOS EM HARDWARE VS. SOFTWARE

- **Proteção contra Acessos Não Autorizados:** Bloqueia tentativas de invasão e acessos indevidos à rede.
- **Filtragem de Tráfego Malicioso:** Pode identificar e bloquear tráfego malicioso, como ataques DDoS (Distributed Denial of Service) ou varreduras de portas.
- **Controle de Políticas de Acesso:** Permite a aplicação de políticas de segurança, controlando o que pode entrar ou sair da rede.
- **Proteção de Dados Sensíveis:** Ajuda a proteger dados internos, garantindo que apenas o tráfego legítimo tenha acesso à rede.

FIREWALLS BASEADOS EM HARDWARE VS. SOFTWARE

Tipo de Firewall	Descrição	Vantagem	Desvantagem	Casos de Uso
Filtro de Pacotes	Analisa cabeçalhos de pacotes	Rápido e simples	Inspeção limitada	Proteção básica
Proxy	Intermediário entre usuário e recurso	Controle detalhado	Pode causar latência	Redes empresariais
Stateful Inspection	Mantém estado das conexões	Balanceia segurança e desempenho	Mais complexo	Empresas de médio porte
Firewall de Aplicação (WAF)	Protege aplicações web	Proteção contra ataques web	Restrito a certos protocolos	Servidores web
Próxima Geração (NGFW)	Inspeção profunda com IDS/IPS	Alta segurança	Custo elevado	Data centers e alta segurança
Firewall de Nuvem	Protege ambientes de nuvem	Escalável	Dependência de conectividade	Ambientes de nuvem

3.

FIREWALL ZONA

Conceitos e utilizando o simulador

FIREWALL DE ZONA

O que é um firewall de zona?

- Um firewall de zona é uma implementação que agrupa interfaces de rede em diferentes zonas de segurança.
- O tráfego entre as interfaces é controlado com base nas políticas definidas para as zonas.

Como funciona?

- Tráfego entre zonas diferentes só é permitido se houver uma política explícita que autorize.O tráfego dentro da mesma zona é, por padrão, permitido.
- **Zonas comuns:**
  - **Inside:** Normalmente a rede interna confiável.
  - **Outside:** Rede não confiável, como a internet.
  - **DMZ (Demilitarized Zone):** Rede parcialmente confiável que hospeda servidores acessíveis externamente (ex: servidores web).

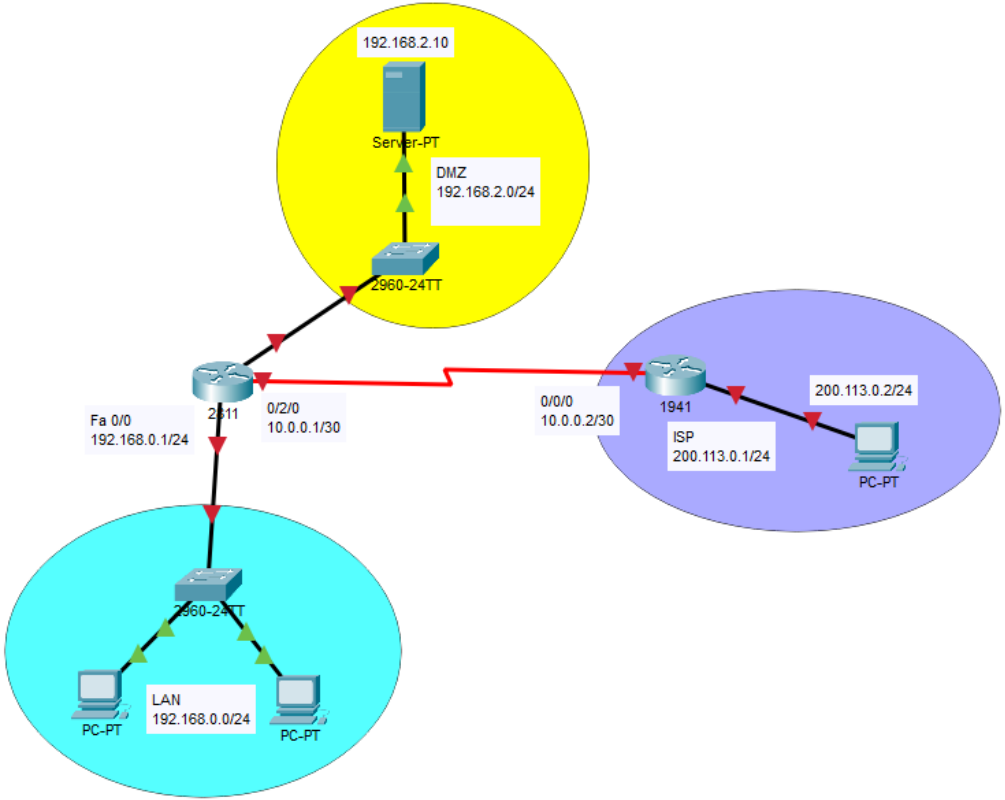
FIREWALL DE ZONA

Conceitos de Zonas de Segurança e Políticas

- **Zonas de Segurança:**
  - **Inside:** Dispositivos internos (ex: PCs internos).
  - **Outside:** Internet ou outra rede não confiável.
  - **DMZ:** Área intermediária, onde servidores públicos ficam isolados da rede interna.

- **Políticas de Tráfego:**
  - Tráfego permitido/negado entre as zonas.
  - **Exemplo:**
    - Permitir tráfego da Inside para a Outside.
    - Bloquear tráfego da Outside para a Inside, exceto por conexões específicas, como HTTP ou HTTPS.

SIMULADOR



- Permitir tráfego da Zona Inside para a Zona Outside (Rede Interna para a Internet)
  - Protocolo permitido: HTTP (porta 80), HTTPS (porta 443), ICMP (ping).
- Permitir tráfego da Zona Outside para a Zona DMZ (Acesso ao servidor web na DMZ)
  - Protocolo permitido: HTTP (porta 80), HTTPS (porta 443).
- Bloquear tráfego da Zona Outside para a Zona Inside (Bloquear conexões diretas da Internet para a Rede Interna)
  - Protocolo bloqueado: Todos, exceto tráfego permitido entre Outside e DMZ.

SIMULADOR - SOLUÇÃO

- zone security inside
- zone security out
- sidezone security dmz

Criação das zonas:
Inside → rede interna;
Outside → internet
Dmz → DMZ

- interface fa0/0
  zone-member security inside
- interface fa0/1
  zone-member security dmz
- interface serial 0/0/0
  zone-member security outside

Atribuição das zonas nas portas de redes.

SIMULADOR - SOLUÇÃO

class-map type inspect match-any inside_to_outside

- match protocol http
- match protocol https
- match protocol icmp

Atribuição das zonas nas portas de redes.

Define a classe dos métodos que serão analisados.
Match-any → qualquer um dos protocolos pode ser correspondidos.
Match-all → todos os critérios devem ser atendidos simultaneamente para que faça a ação

class-map type inspect match-any outside_to_dmz

- match protocol http
- match protocol https

Nome dado a classe, podemos utilizar qualquer nome

SIMULADOR - SOLUÇÃO

- policy-map type inspect inside_to_outside_policy
  - class type inspect inside_to_outside
    - Inspect
- policy-map type inspect outside_to_dmz_policy
  - class type inspect outside_to_dmz
    - inspect

Define uma política de inspeção de tráfego

Aplica a class-map previamente definida dentro desta política

inspect: Permite o tráfego e realiza a inspeção de estado. Pacotes de retorno de conexões válidas são permitidos.
pass: Permite o tráfego, mas não realiza a inspeção de estado. O tráfego de retorno será bloqueado a menos que haja uma regra separada.
drop: Bloqueia explicitamente o tráfego que corresponde à class-map

Nome dado a classe, podemos utilizar qualquer nome

SIMULADOR - SOLUÇÃO

- **zone-pair security** inside_to_outside **source inside destination outside**
  - **service-policy type inspect** inside_to_outside_policy

Aplica uma política de inspeção a esse zone-pair. A política de inspeção (chamada inside_to_outside_policy neste caso) define como o tráfego será tratado entre as duas zonas. Essa política especifica que o tráfego será inspecionado para garantir que apenas conexões legítimas sejam permitidas.

Um zone-pair: define a relação entre duas zonas de segurança.

source inside: Define a zona de origem.

destination outside: Define a zona de destino.

- **zone-pair security outside_to_dmz source outside destination dmz**
  - **service-policy type inspect outside_to_dmz_policyexit**

SIMULADOR - TESTES

Teste de conectividade básico:

- Ping da zona inside para a outside (rede interna → Internet) – Tem que funcionar.
- Ping da Outside para a Inside – Não pode funcionar

Teste de Navegação HTTP/HTTPS

- Inside para Outside – Tem que funcionar (obs. Coloque um servidor WEB)
- Outside para Inside – Não pode funcionar

Acesso a DMZ:

- Outside para DMZ – Tem que funcionar
- Inside para DMZ – não pode funcionar

3.

EXERCÍCIOS

Usando packet tracer

OBRIGADO!