Listas de Controle de Acesso

Prefácio

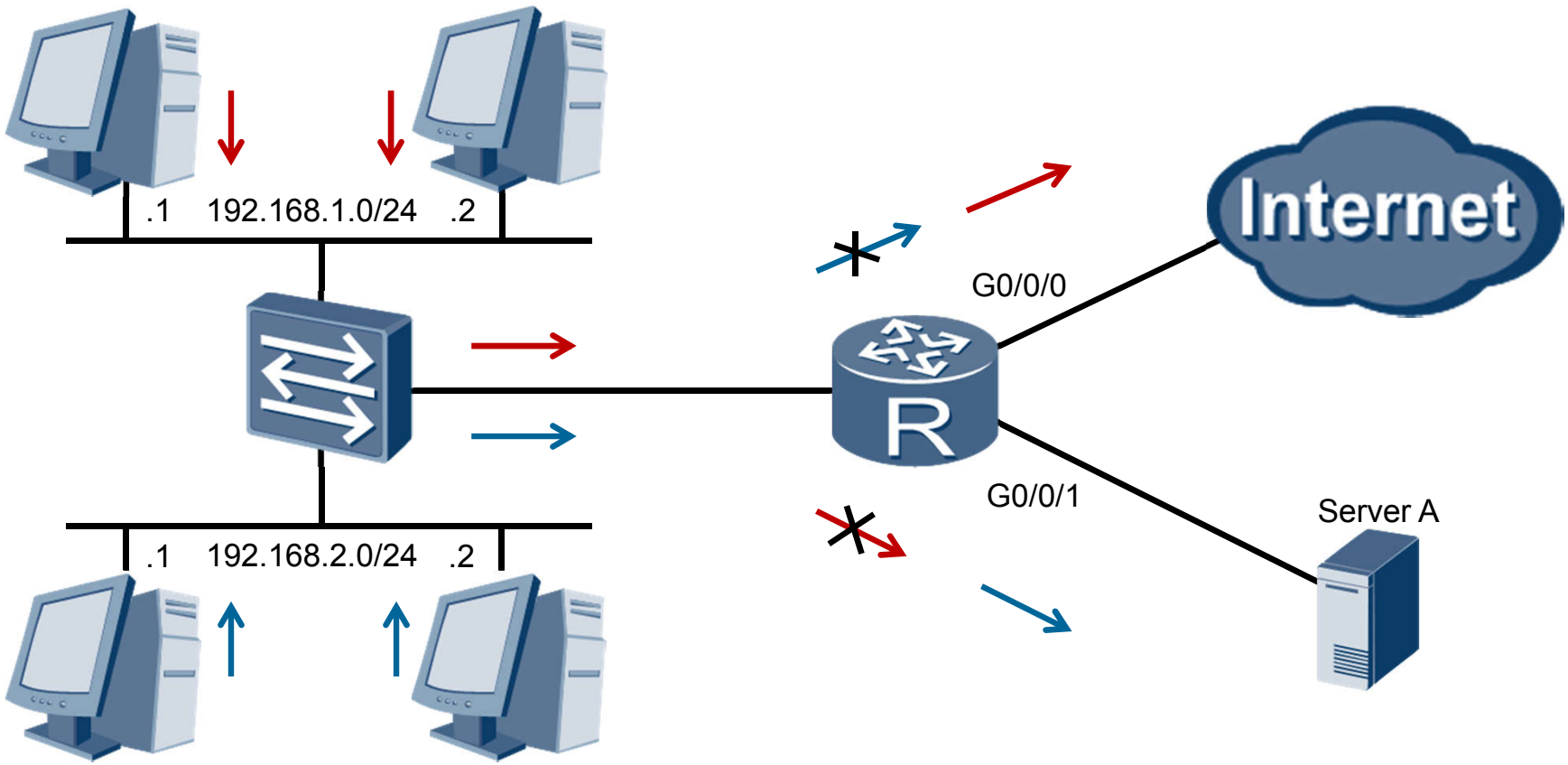
Muitas tecnologias e protocolos dependem de Listas de Controle de Acesso (Access Control Lists – ACL) para aprimorar o gerenciamento e filtragem de tráfego como parte de medidas de segurança ou requerimentos de aplicações. A implantação de ACL como suporte a outras tecnoogias, e como uma forma de segurança, são de suma importância de serem entendidas.

Objetivos

Após completer esta seção os estudantes serão capazes de:

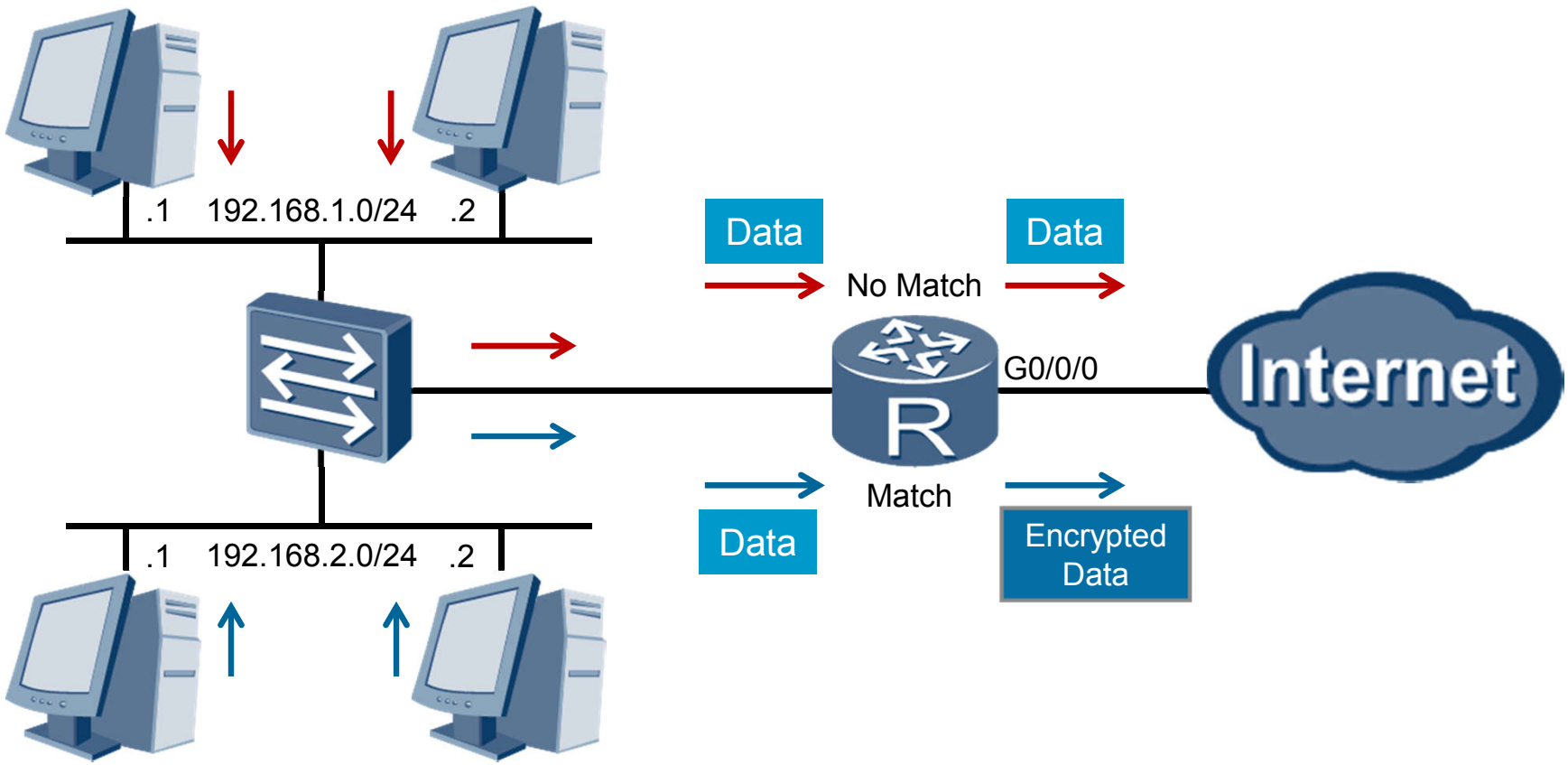
- Descrever as aplicações de ACL em uma rede empresarial.
- Explicar o processo de decisão que ocorre em uma ACL.
- Implementar ACLs básicas e avançadas.

Filtragem de Tráfego



- Pacotes são filtrados com base em endereços e parâmetros.
- Regras definem se pacotes são permitidos ou negados.

Filtragem de Tráfego Interessante



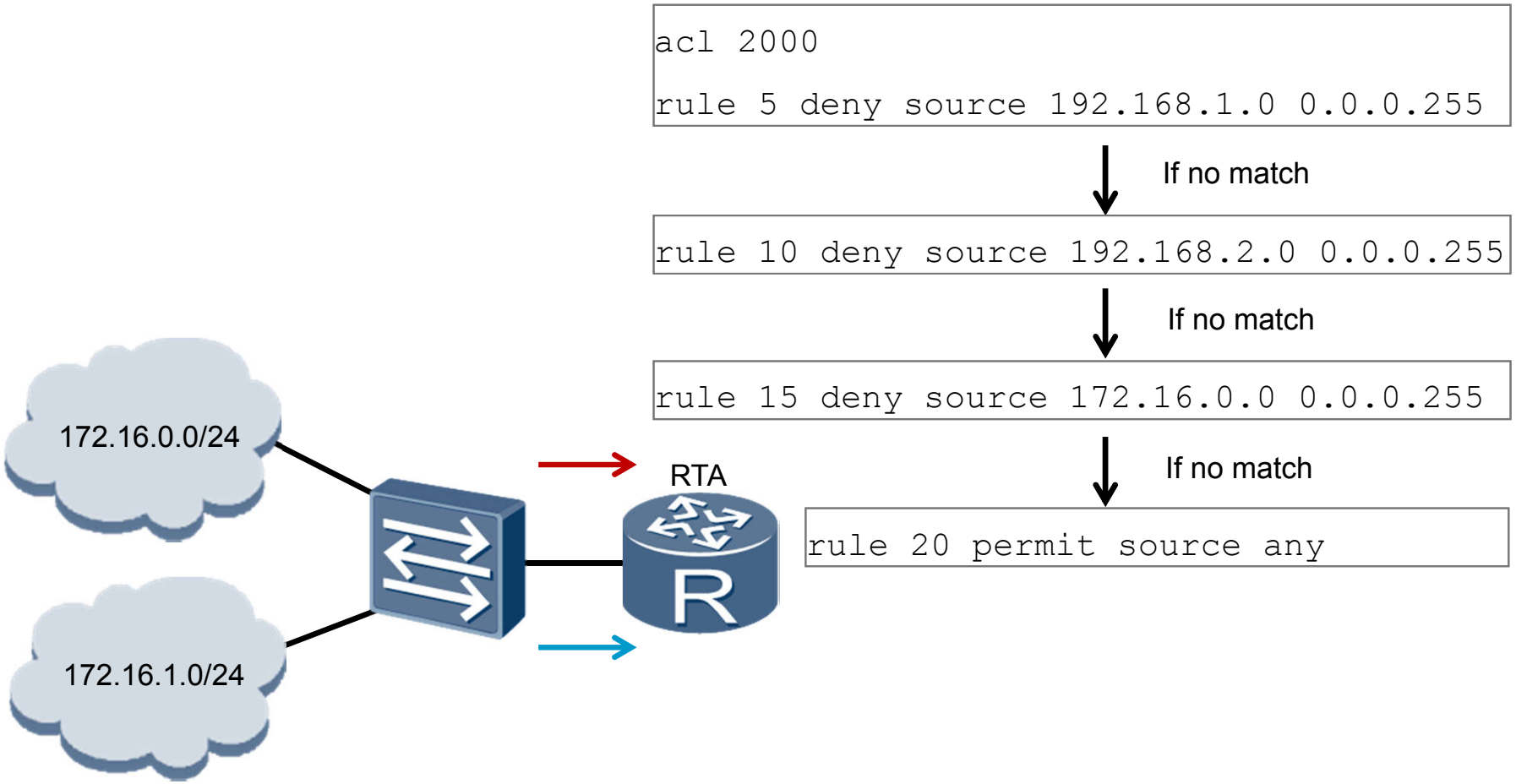
- Pacotes podem ser filtrados para manipular comportamento e ações.
- Parâmetros e encaminhamento podem ser alterados.

Tipos de ACL

Tipos	Intervalo	Parâmetros
Básica	2000-2999	IP de origem
Avançada	3000-3999	Ip de origem e destino, protocol, porta de origem e destino
L2	4000-4999	Endereço MAC

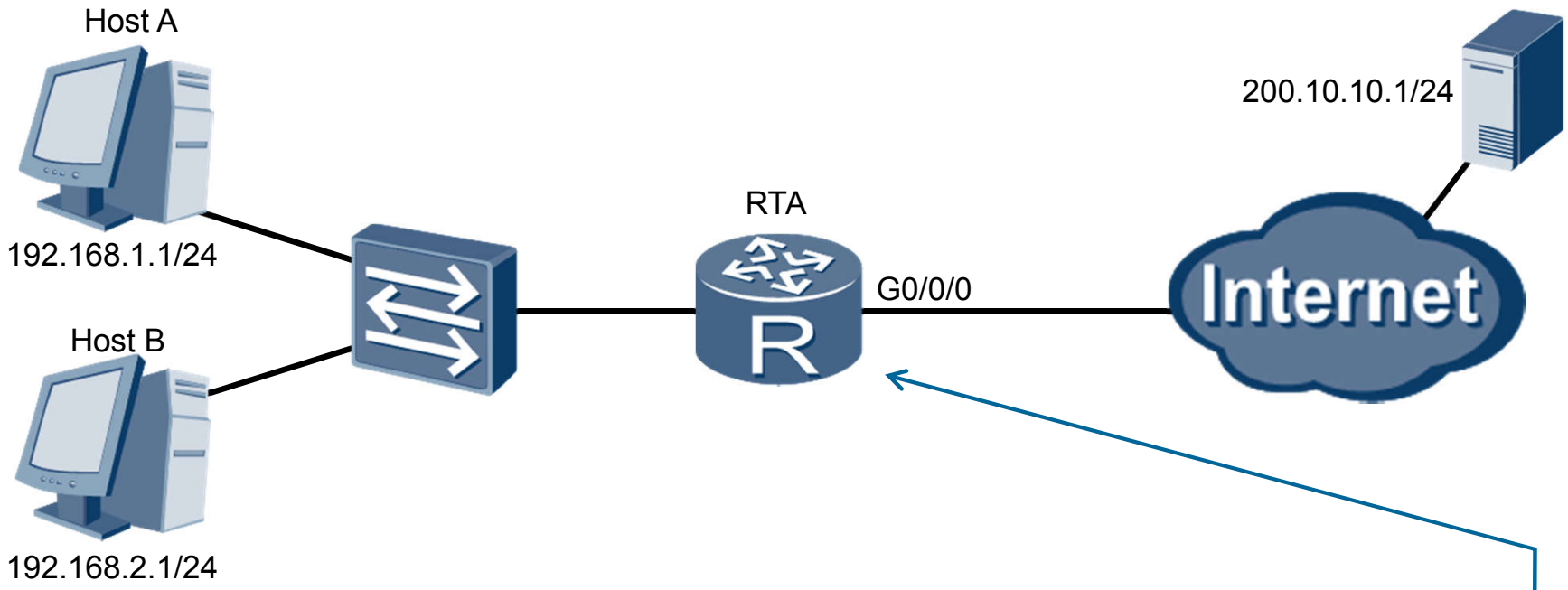
- Três formas de ACL podem ser aplicadas em roteadores da seré AR2200.
- Parâmetros filtrados variam de acordo com o tipo de ACL.

Processo de Decisão na ACL



- Regra são usadas para gerenciar o processo de decisão em cada ACL.

ACL Básica




```
[RTA]acl 2000
[RTA-acl-basic-2000]rule deny source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255
[RTA]interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
```

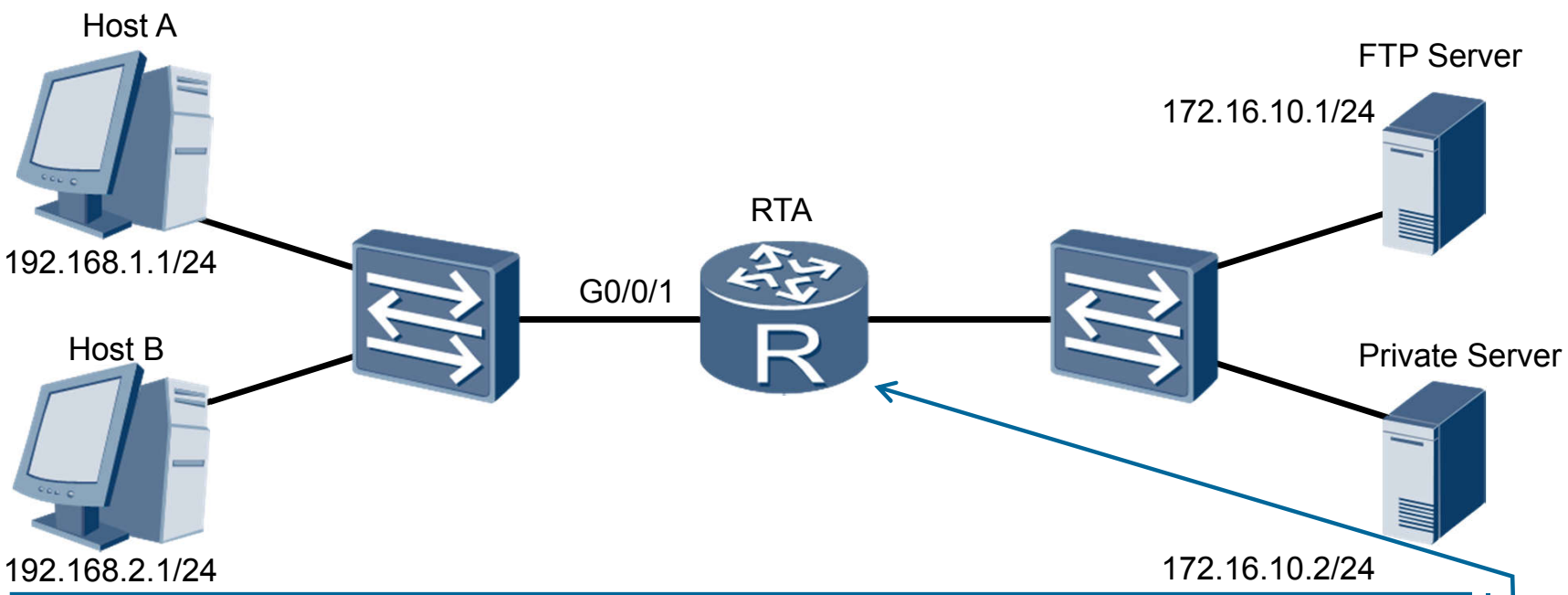
Validação da Configuração

```
Host A> ping 200.10.10.1
Ping 200.10.10.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
...
```

```
[RTA]display acl 2000
Basic ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 192.168.1.0 0.0.0.255 (5 matches)
 rule 10 permit source 192.168.2.0 0.0.0.255
```

- As regras e ordem de correspondência podem ser verificadas em cada ACL.
- ACL básicas analisam o IP de origem do cabeçalho do pacote IP.

ACL Avançada



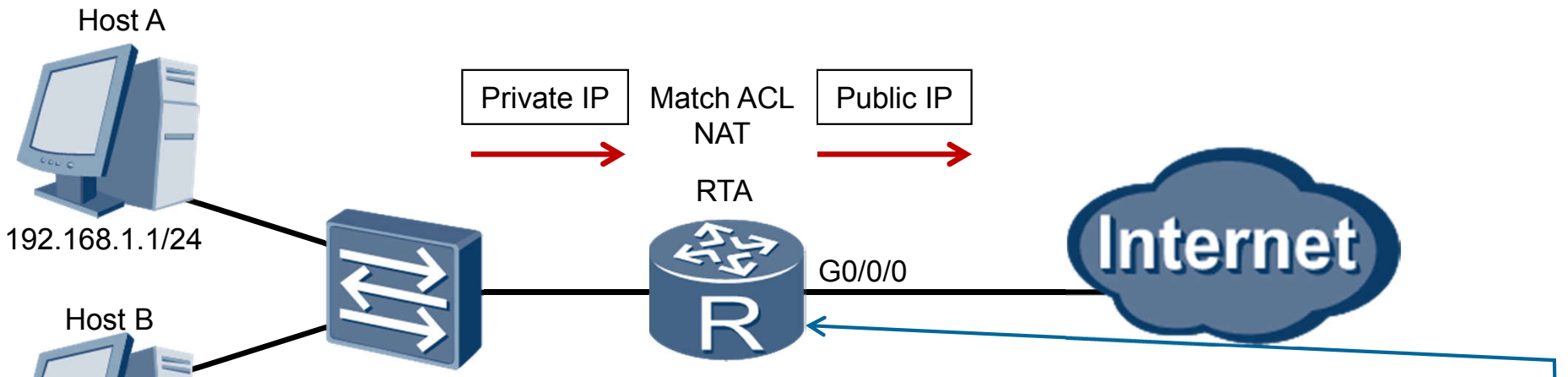

```
[RTA]acl 3000
[RTA-acl-adv-3000]rule deny tcp source 192.168.1.0 0.0.0.255
destination 172.16.10.1 0.0.0.0 destination-port eq 21
[RTA-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255
destination 172.16.10.2 0.0.0.0
[RTA-GigabitEthernet0/0/1]traffic-filter inbound acl 3000
```

Validação da Configuração

```
[RTA]display acl 3000
Advanced ACL 3000, 2 rules
Acl's step is 5
rule 5 deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0
destination-port eq ftp
rule 10 deny ip source 192.168.2.0 0.0.0.255 destination 172.16.10.2 0
```

- ACL avançadas tem número entre 3000-3999 e permitem a filtragem de mais parâmetros.

Aplicação de ACL: NAT




```
[RTA] nat address-group 1 202.110.10.8 202.110.10.15
[RTA] nat address-group 2 202.115.60.1 202.115.60.30
[RTA] acl 2000
[RTA-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000] acl 2001
[RTA-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[RTA-acl-basic-2001] interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0] nat outbound 2000 address-group 1
[RTA-GigabitEthernet0/0/0] nat outbound 2001 address-group 2
```

Resumo

- As ACL avançadas são capazes de filtram analisando quais atributos?
- Uma vez que uma regra em uma ACL é correspondida, o que ocorre?

Thank you

www.huawei.com