



Preventing Traffic with Spoofed Source IP Addresses in MikroTik



Presented by
Md. Abdullah Al Naser
Sr. Systems Specialist
MetroNet Bangladesh Ltd
Founder, mn-LAB
info@mn-lab.net

Internet Routing Security

The routing system of the Internet is vulnerable to many security threats such as:



Prefix Hijacks



Route Leaks



IP Address Spoofing

Internet Routing Security

The routing system of the Internet is vulnerable to many security threats such as:



Prefix Hijacks

Control Plane



Route Leaks

Control Plane

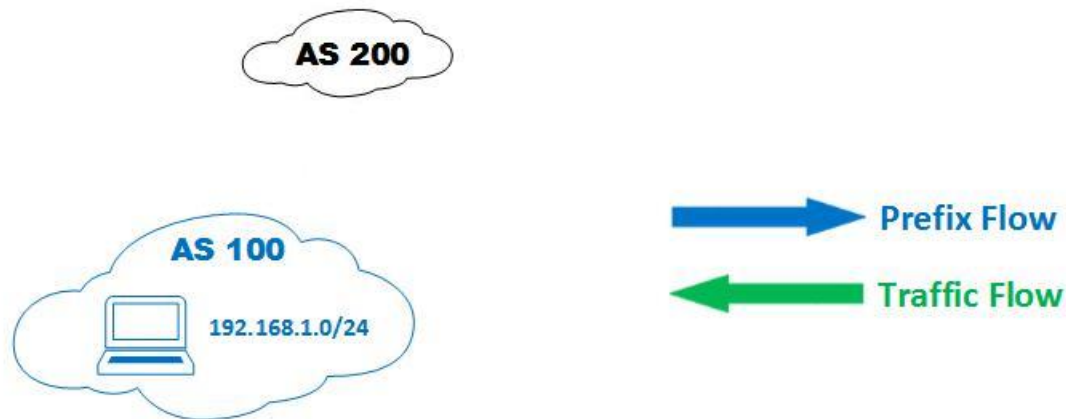


IP Address Spoofing

Data Plane

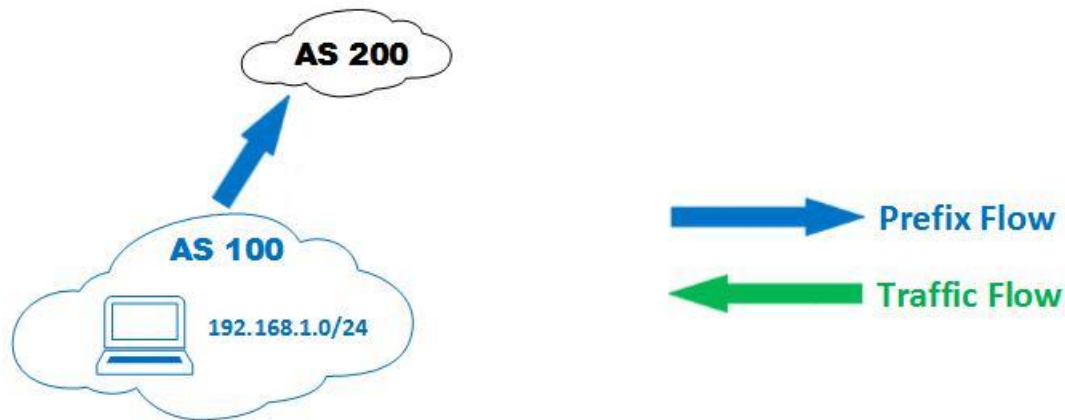
Internet Routing Security

Prefix Hijacks



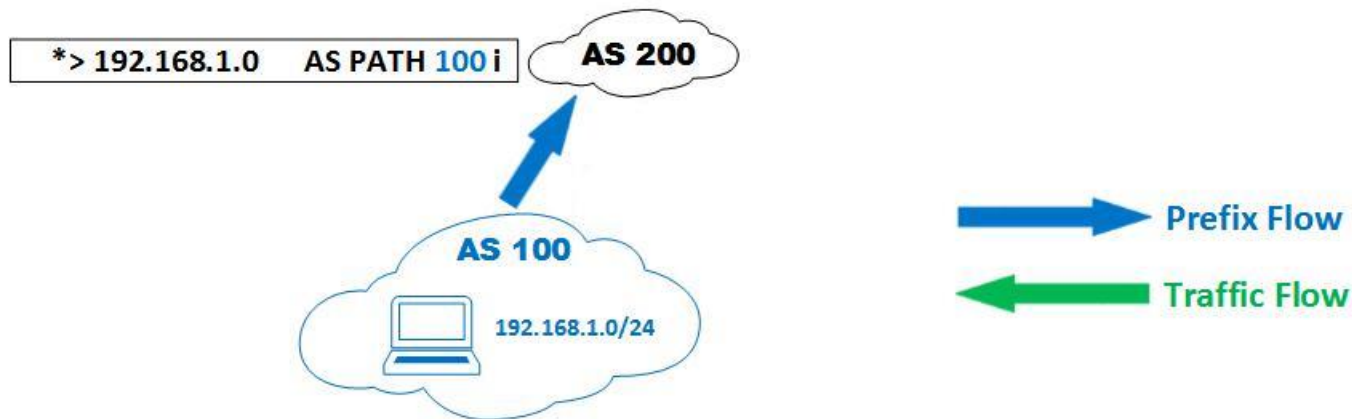
Internet Routing Security

Prefix Hijacks



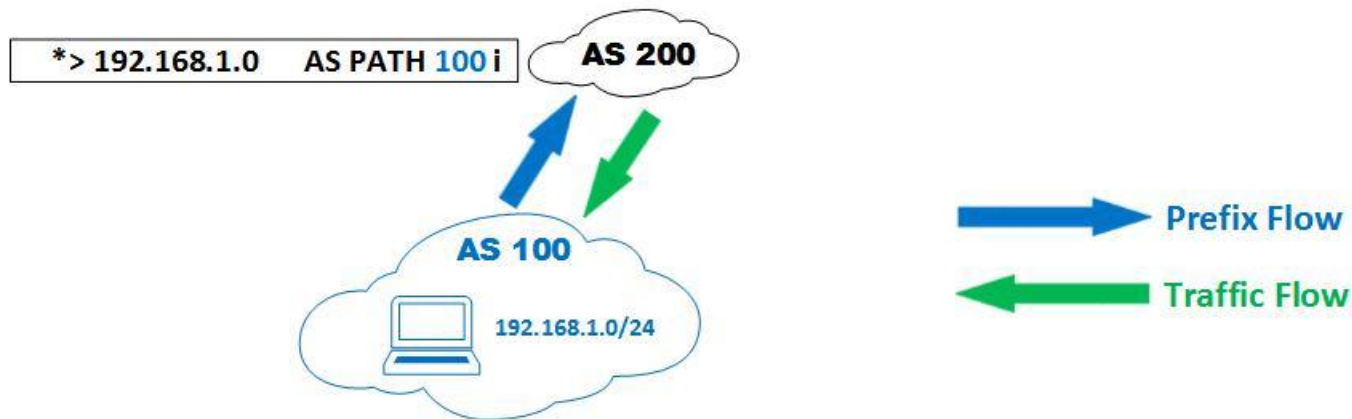
Internet Routing Security

Prefix Hijacks



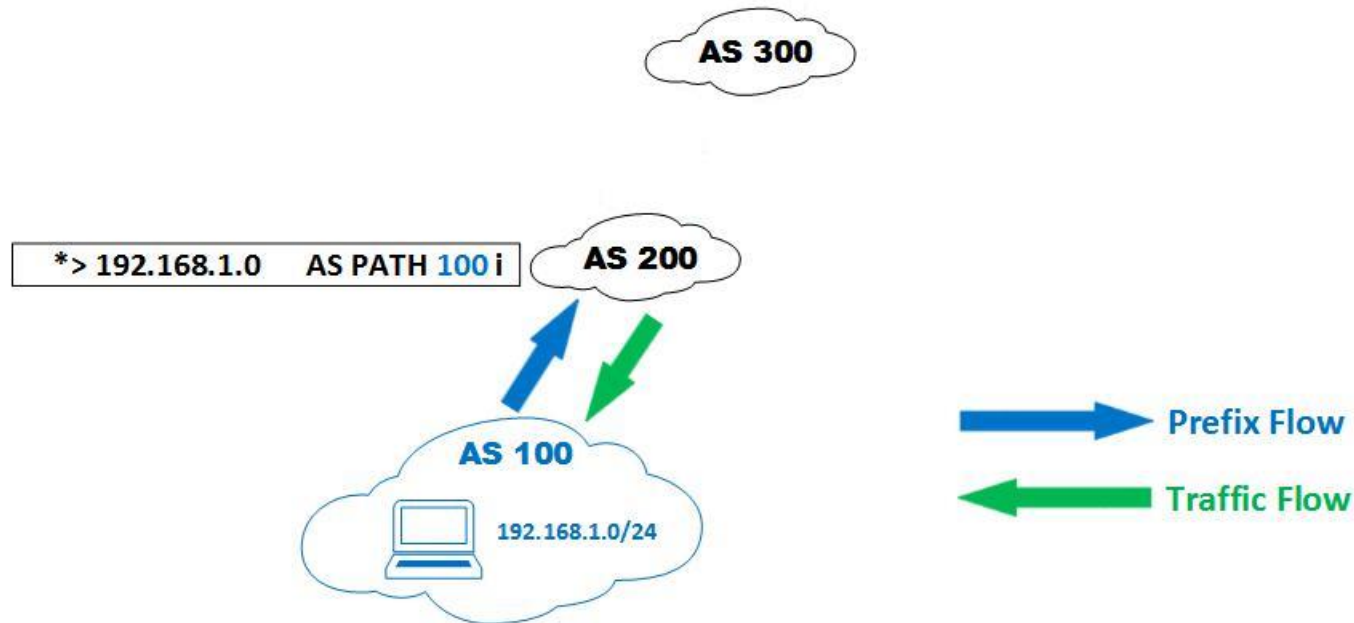
Internet Routing Security

Prefix Hijacks



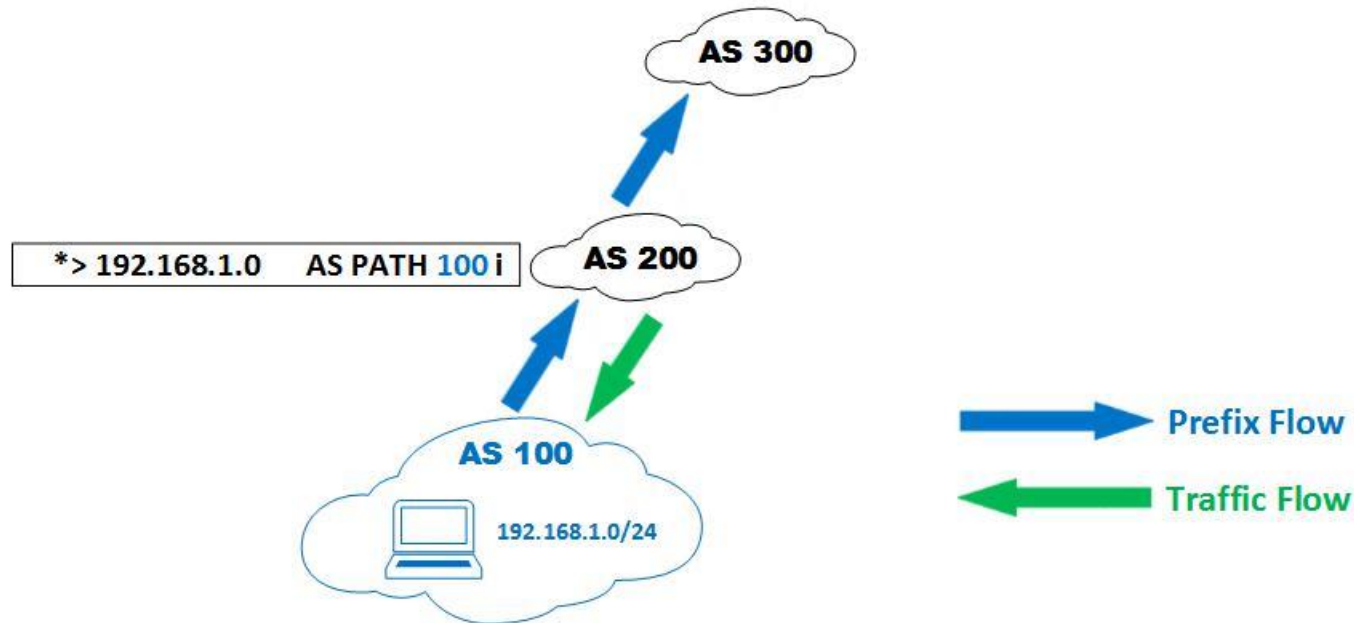
Internet Routing Security

Prefix Hijacks



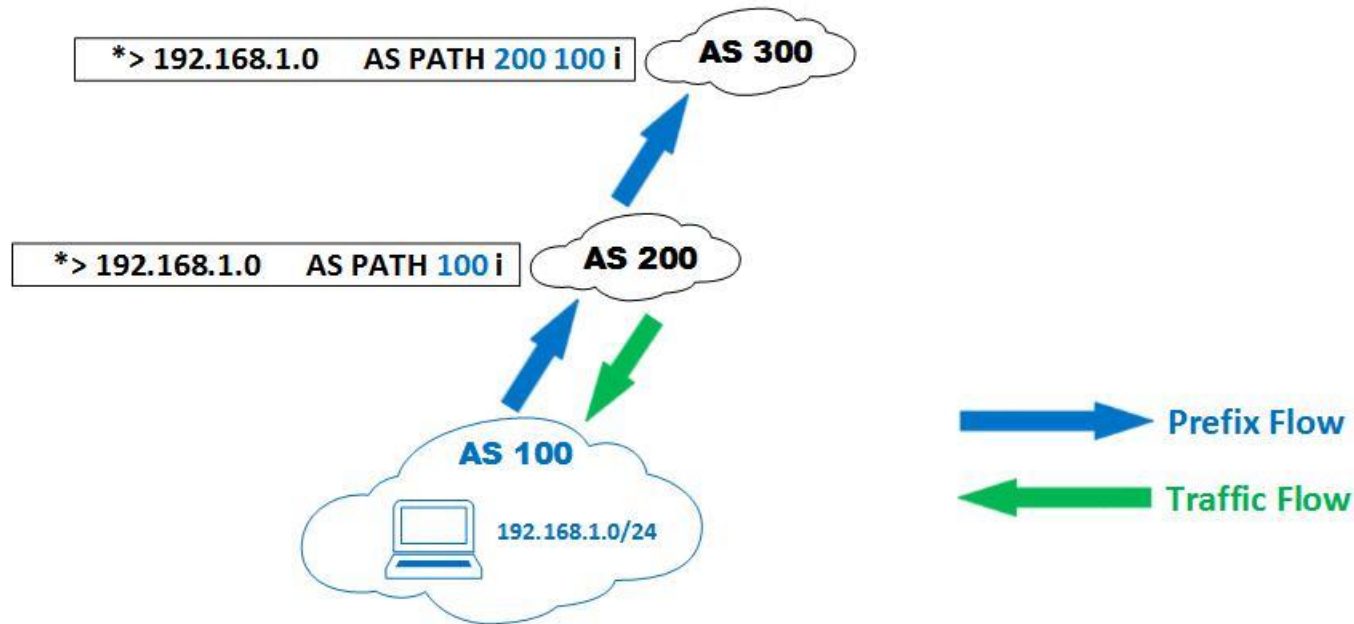
Internet Routing Security

Prefix Hijacks



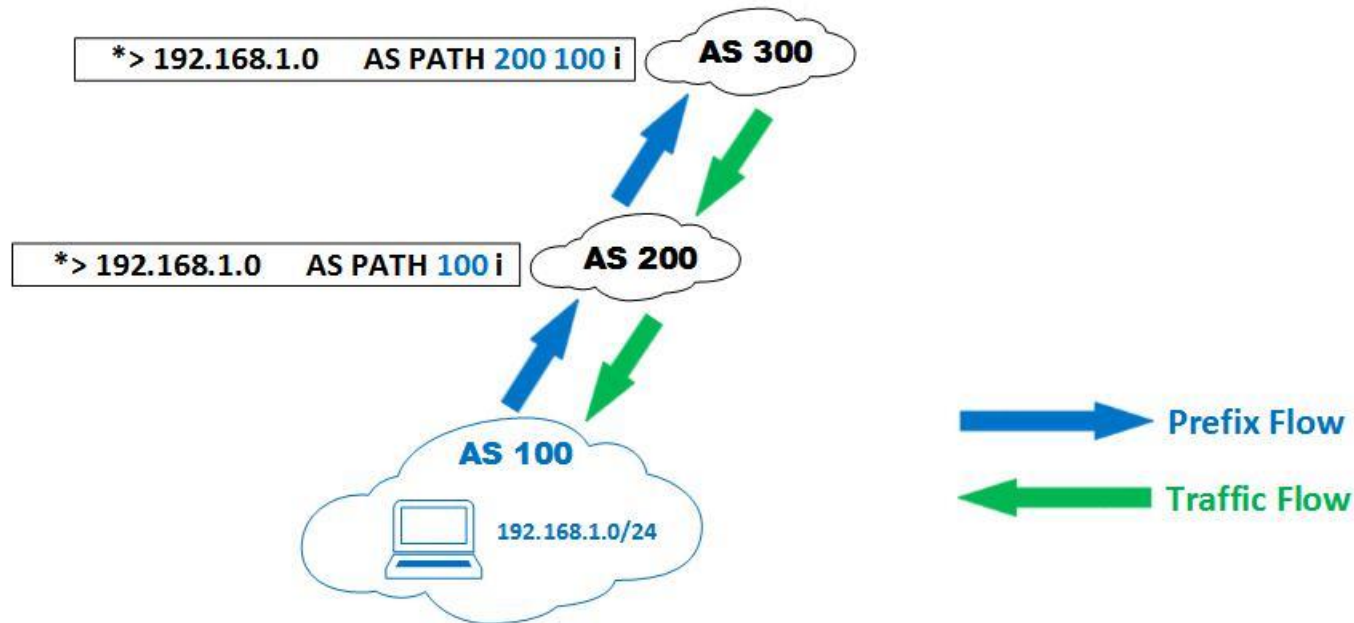
Internet Routing Security

Prefix Hijacks



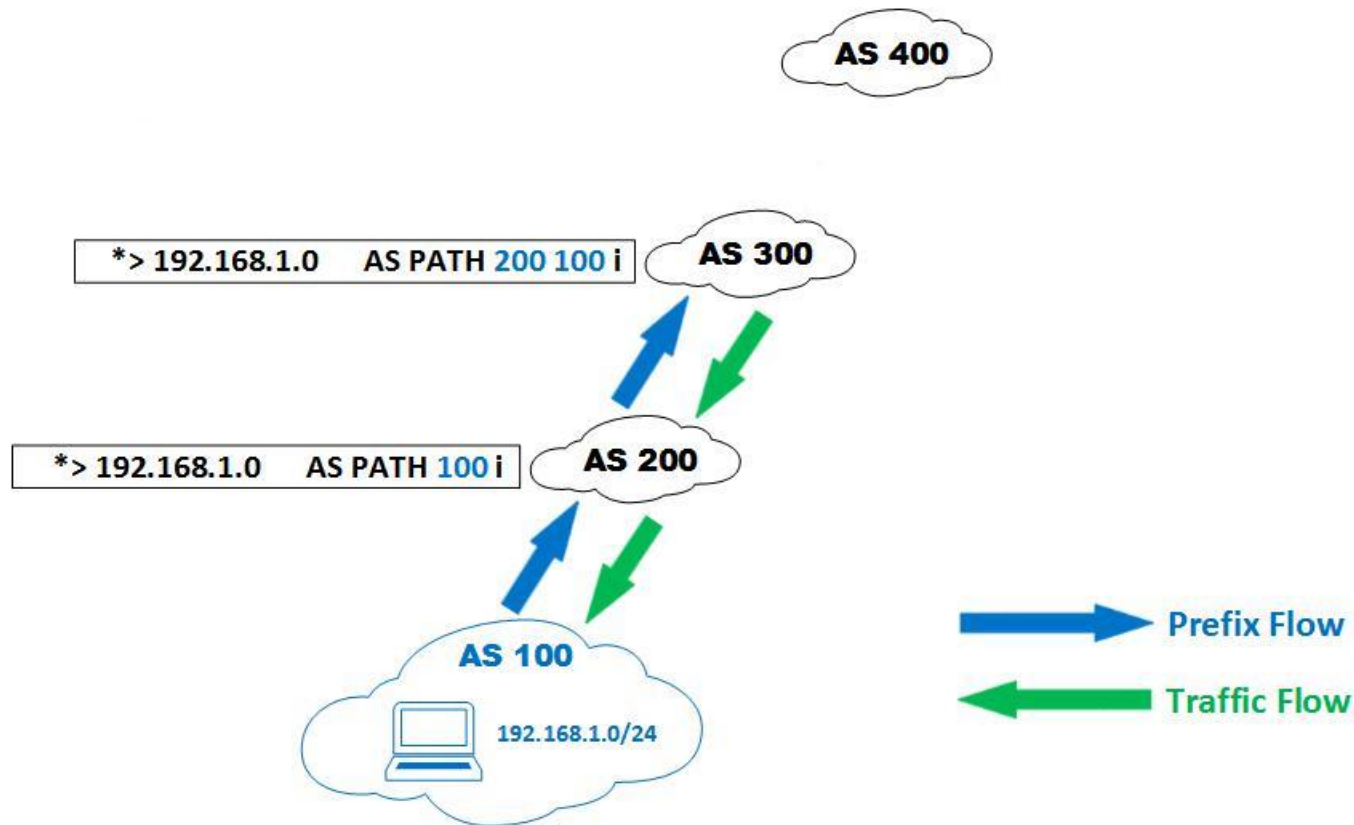
Internet Routing Security

Prefix Hijacks



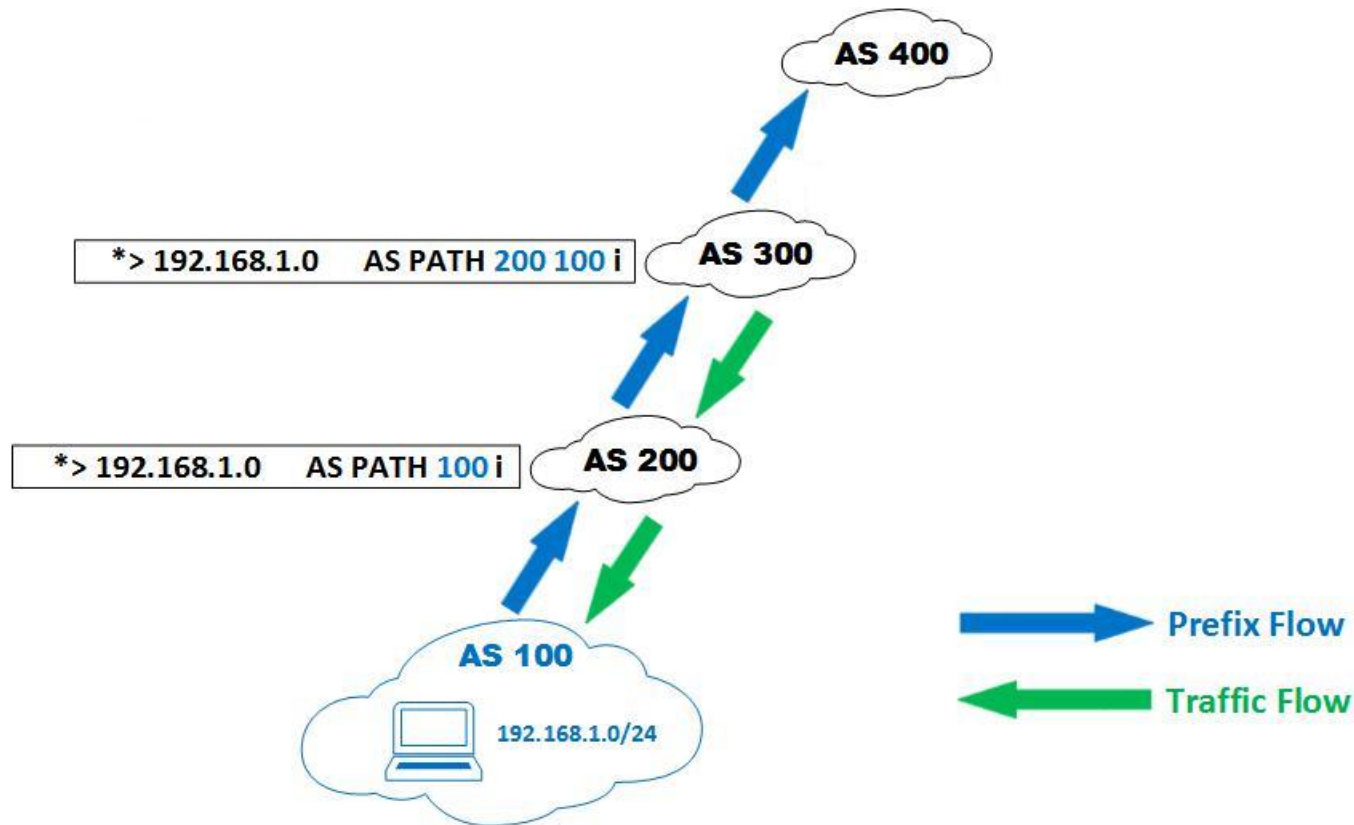
Internet Routing Security

Prefix Hijacks



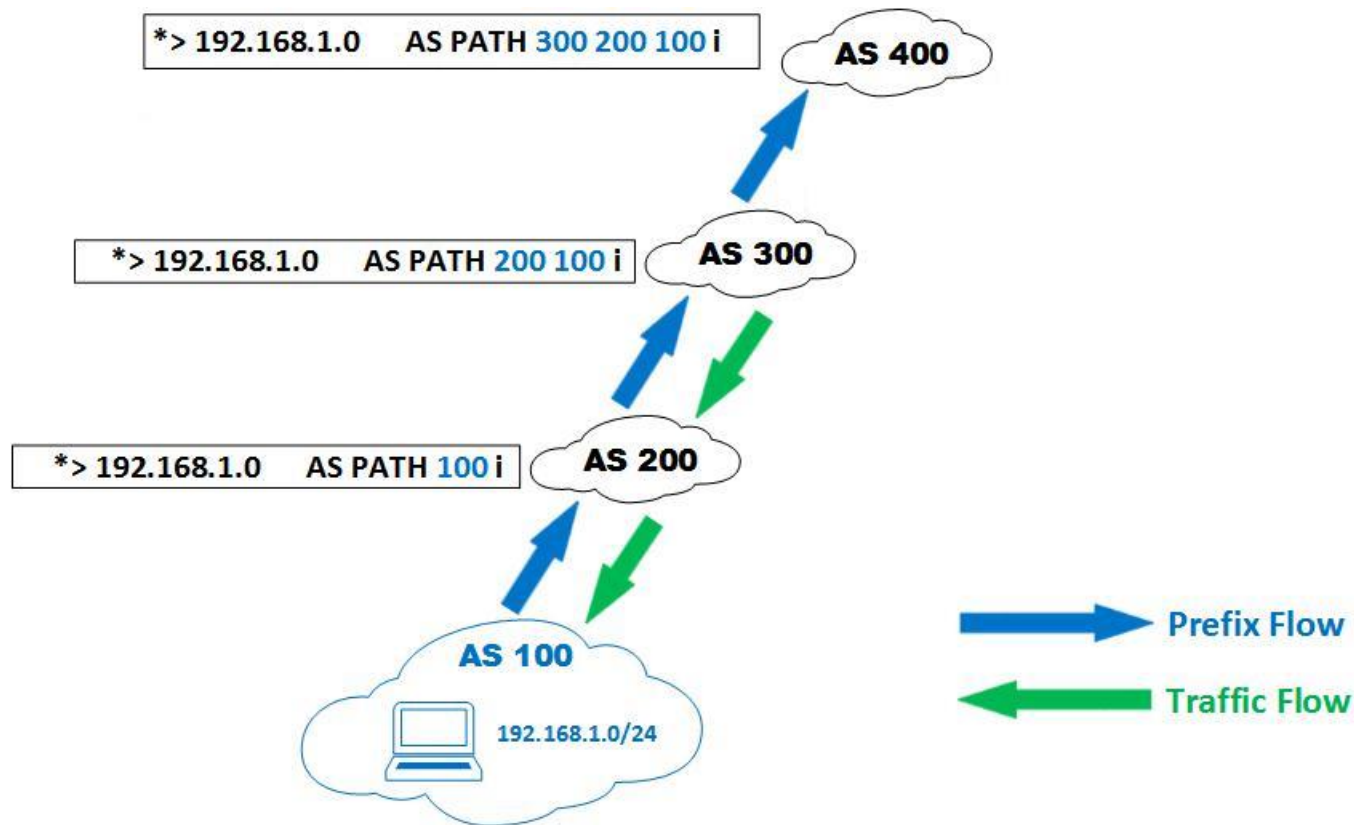
Internet Routing Security

Prefix Hijacks



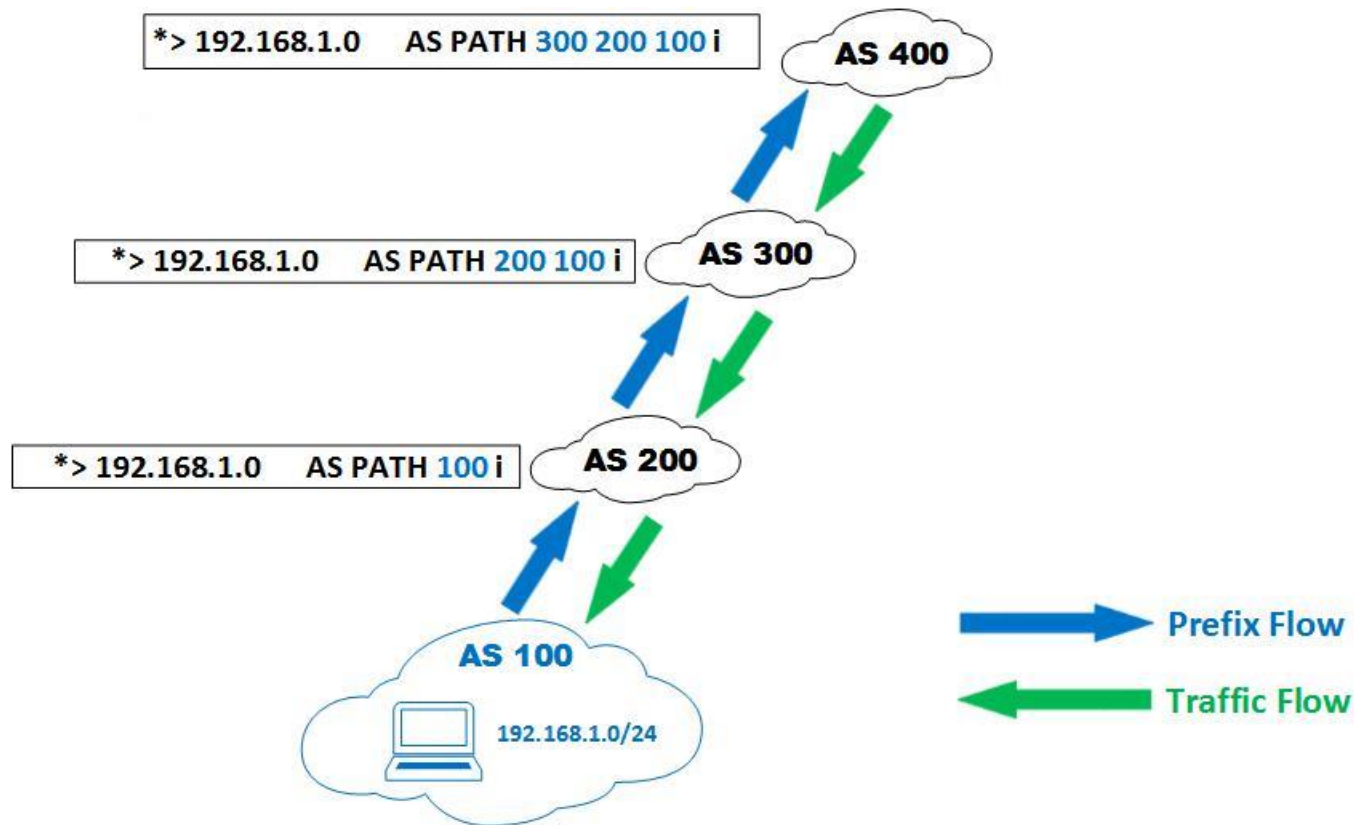
Internet Routing Security

Prefix Hijacks



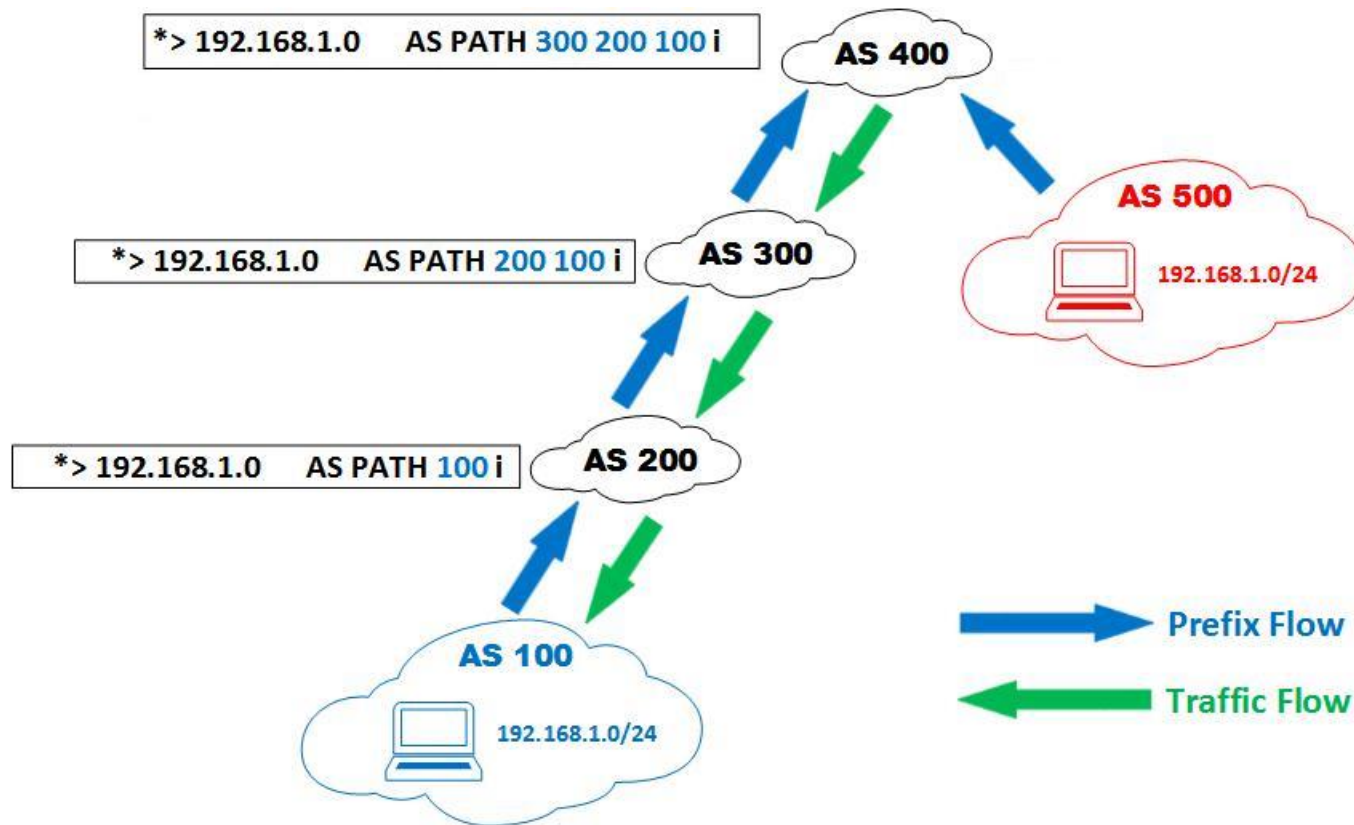
Internet Routing Security

Prefix Hijacks



Internet Routing Security

Prefix Hijacks

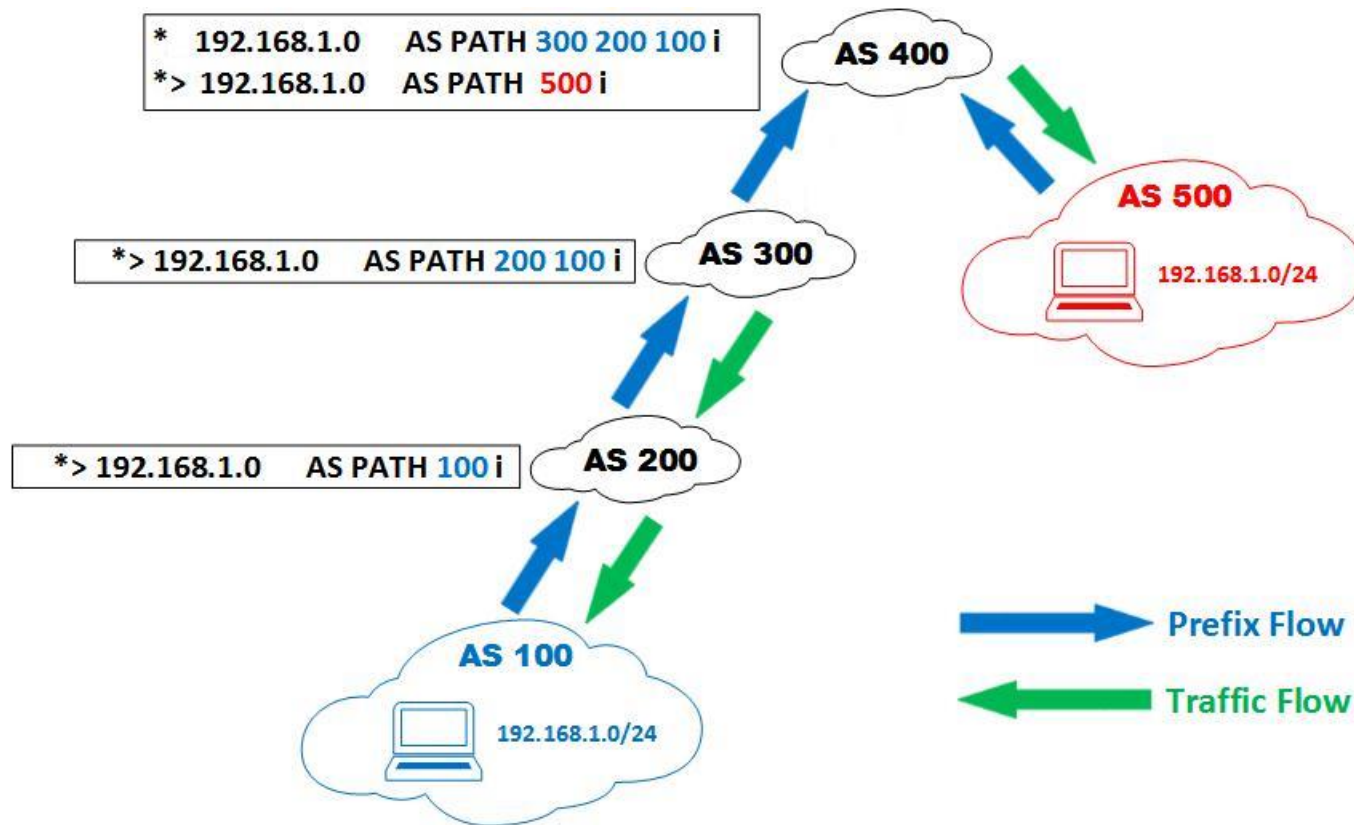


Prefix Hijacks



Internet Routing Security

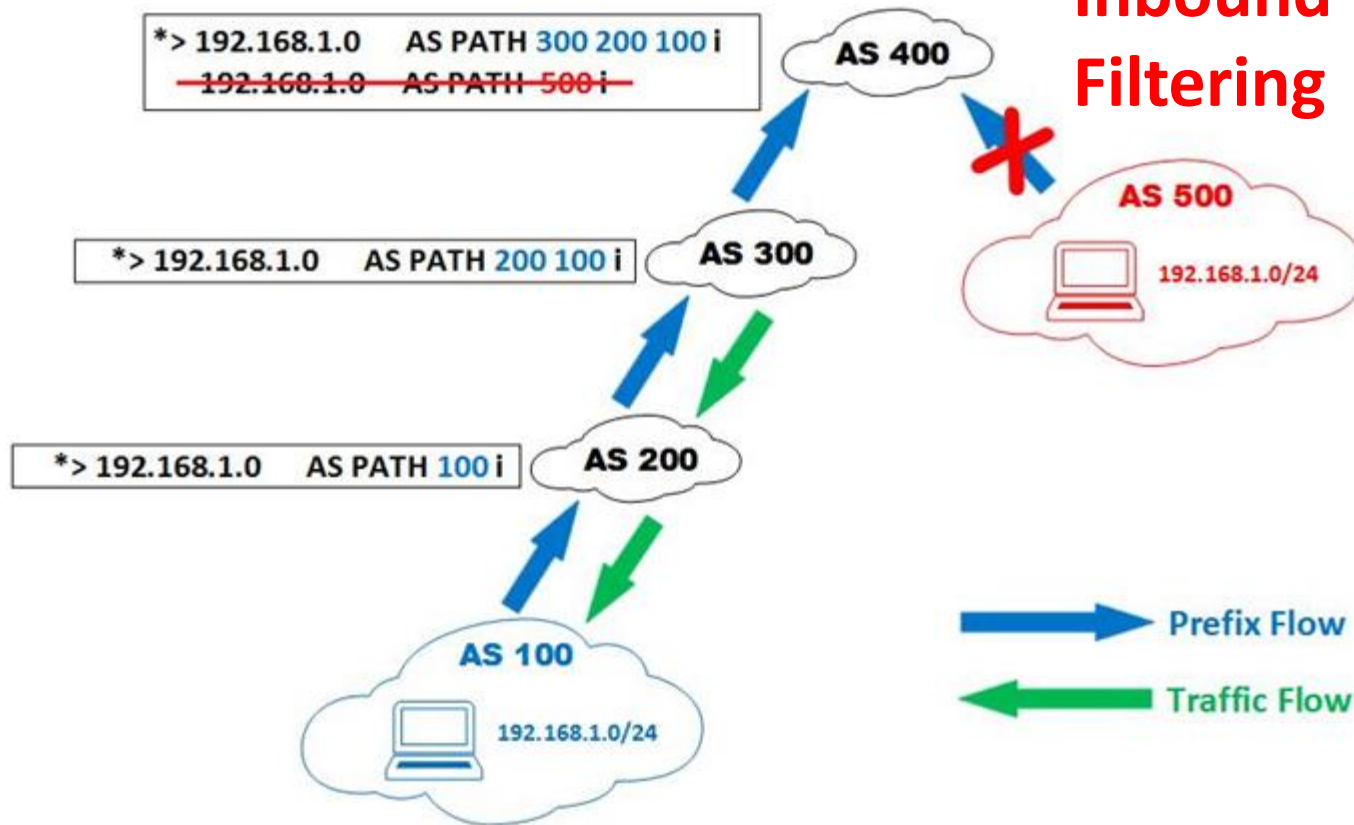
Prefix Hijacks



Internet Routing Security

Prefix Hijacks

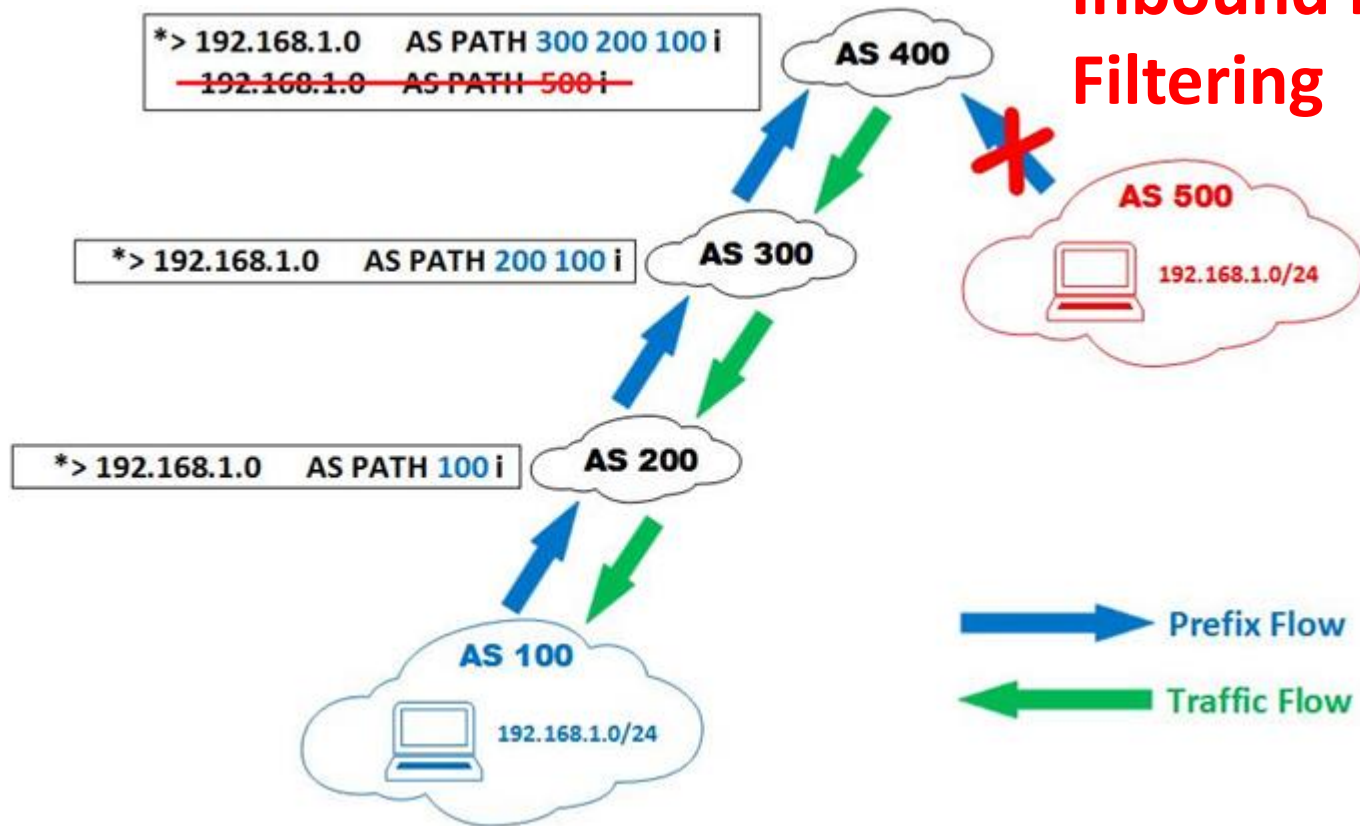
Solution:
Inbound Prefix
Filtering



Internet Routing Security

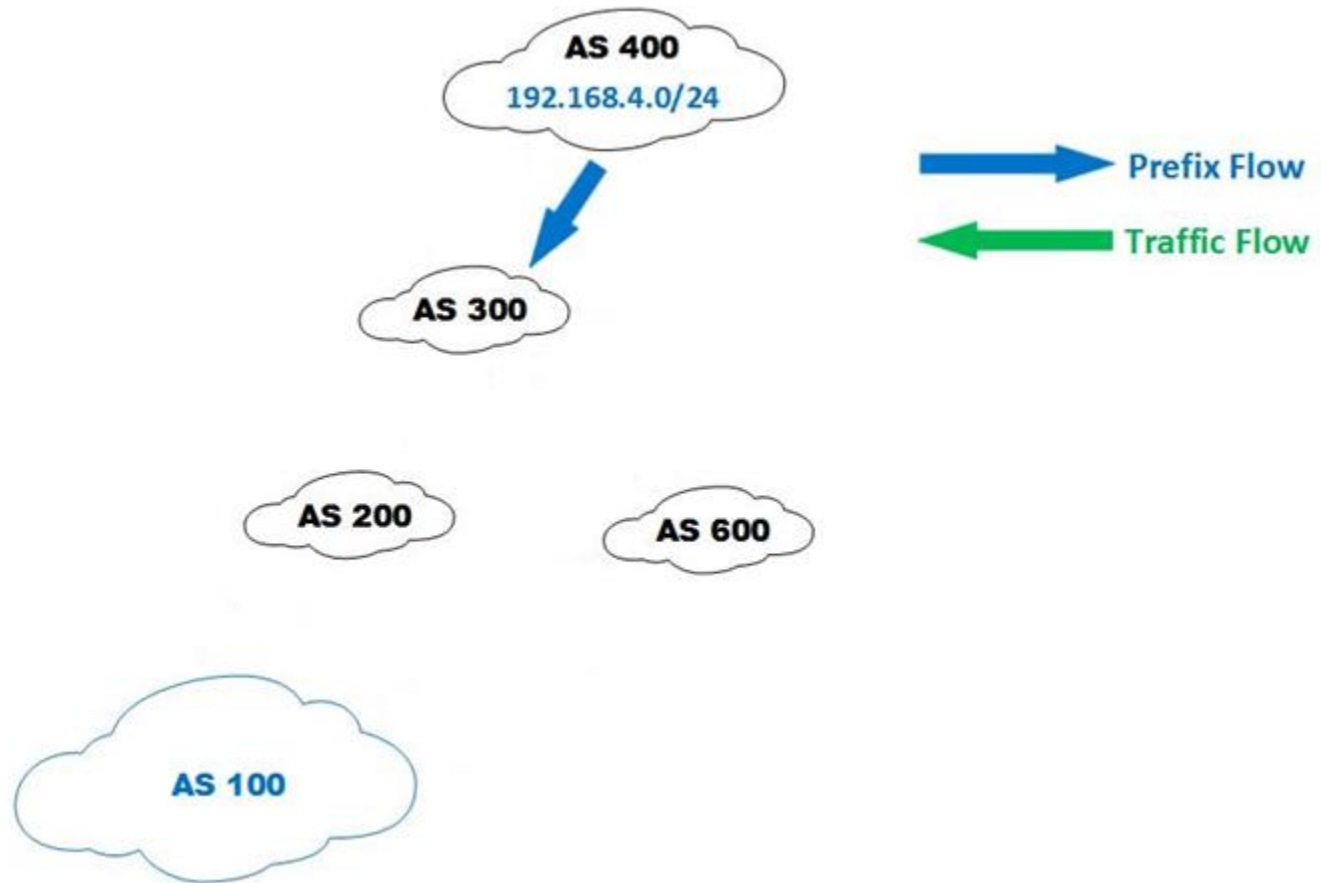
Prefix Hijacks

Solution:
Inbound Prefix
Filtering



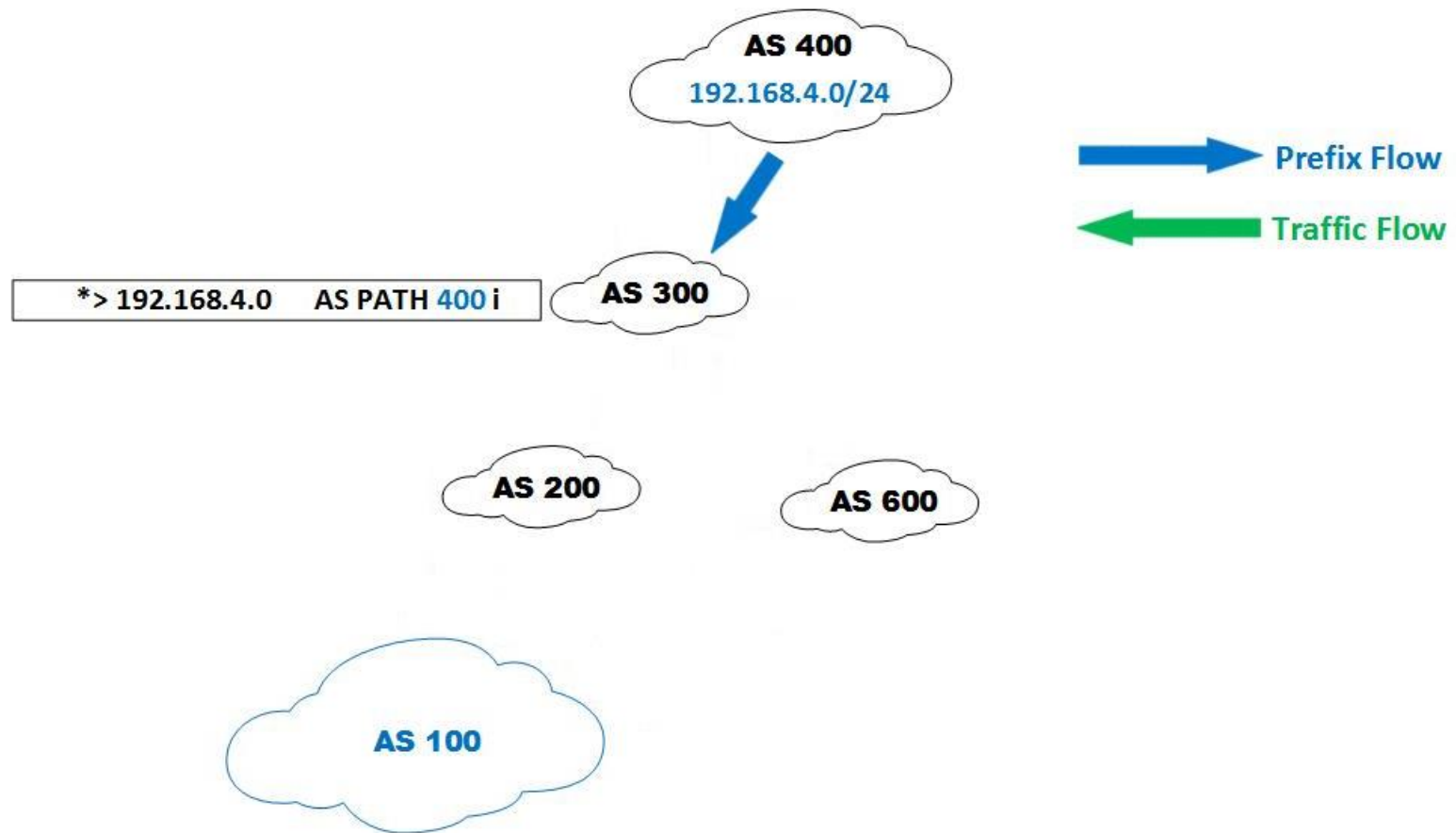
Internet Routing Security

Route Leaks



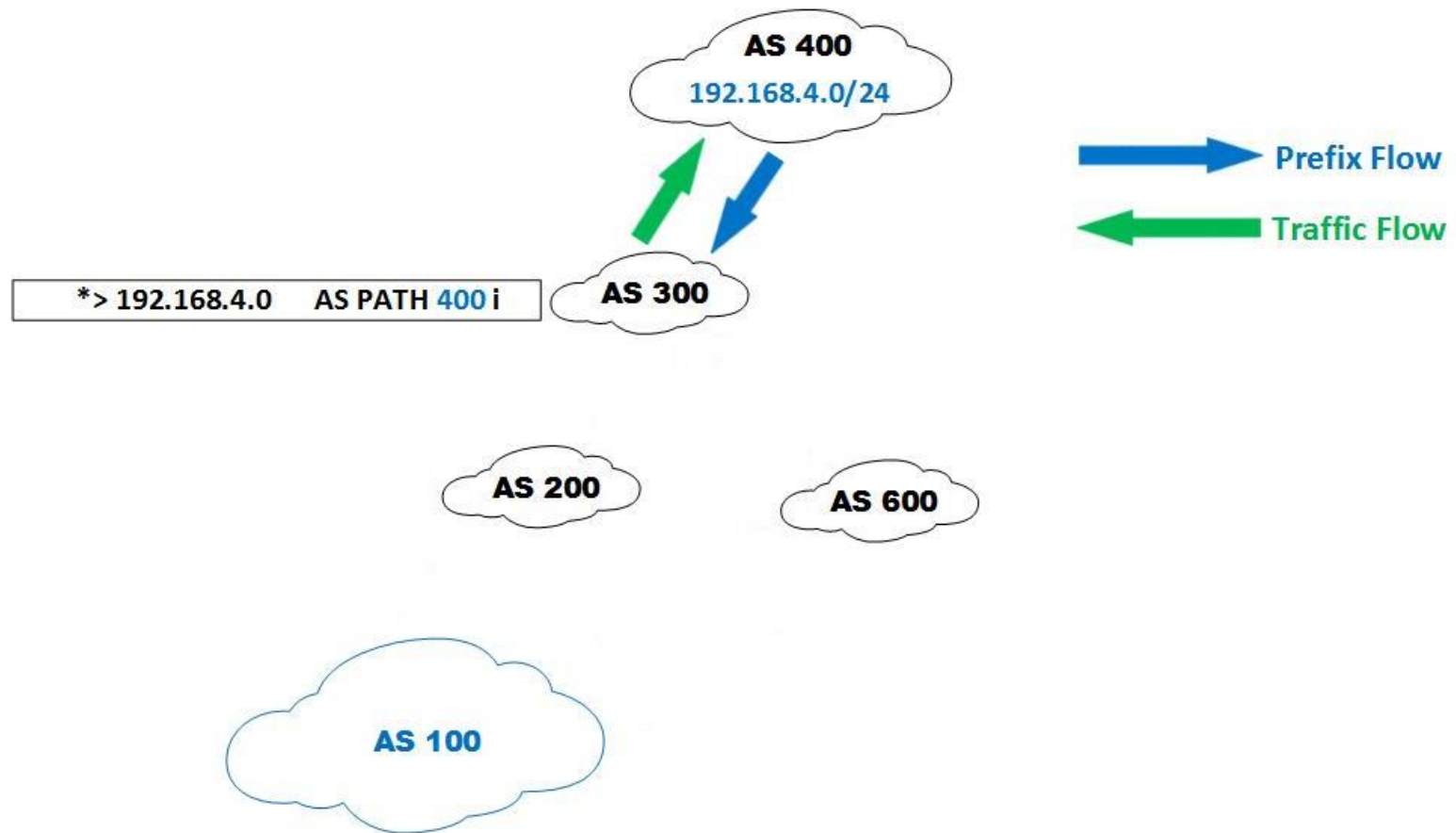
Internet Routing Security

Route Leaks



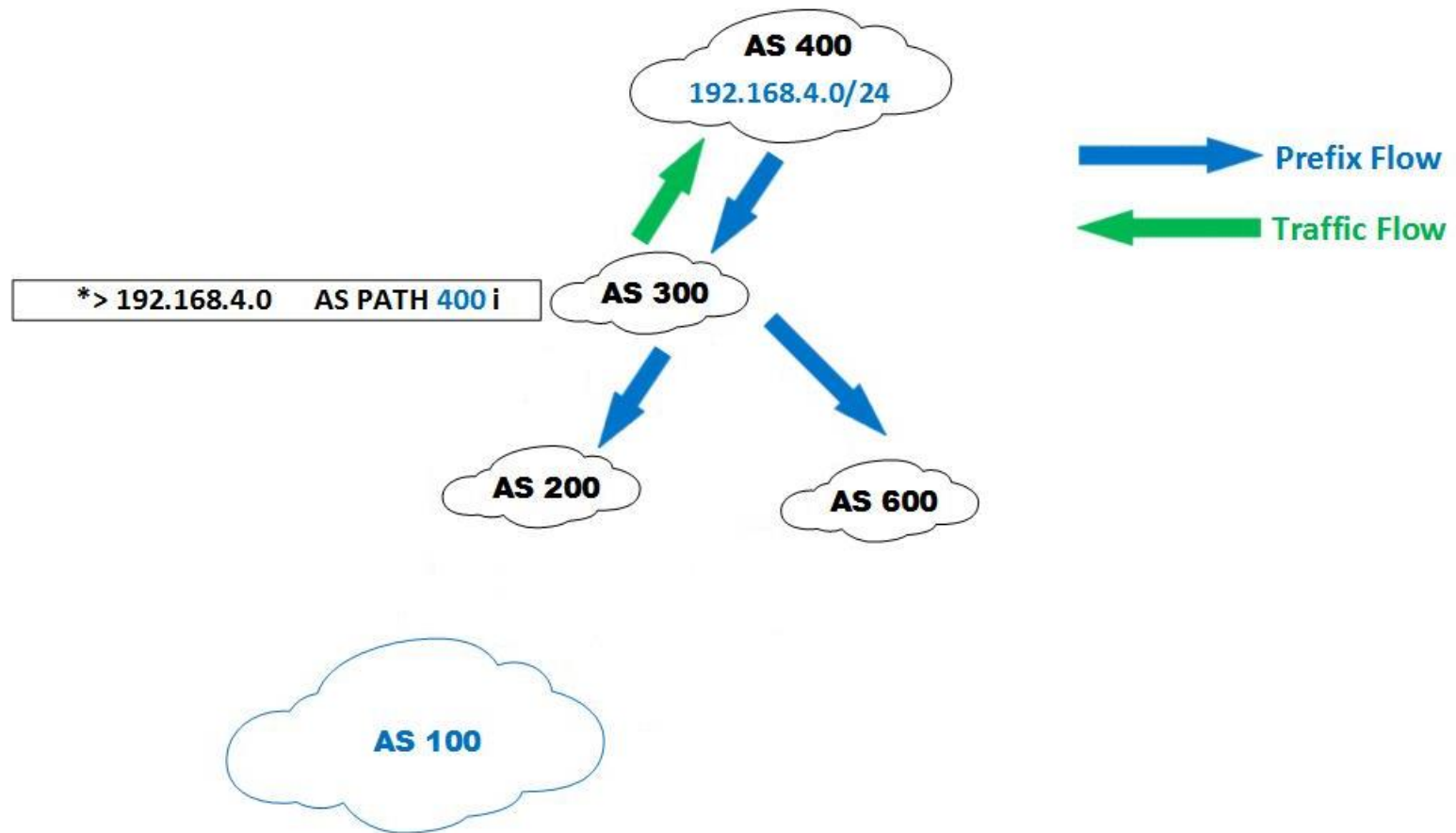
Internet Routing Security

Route Leaks



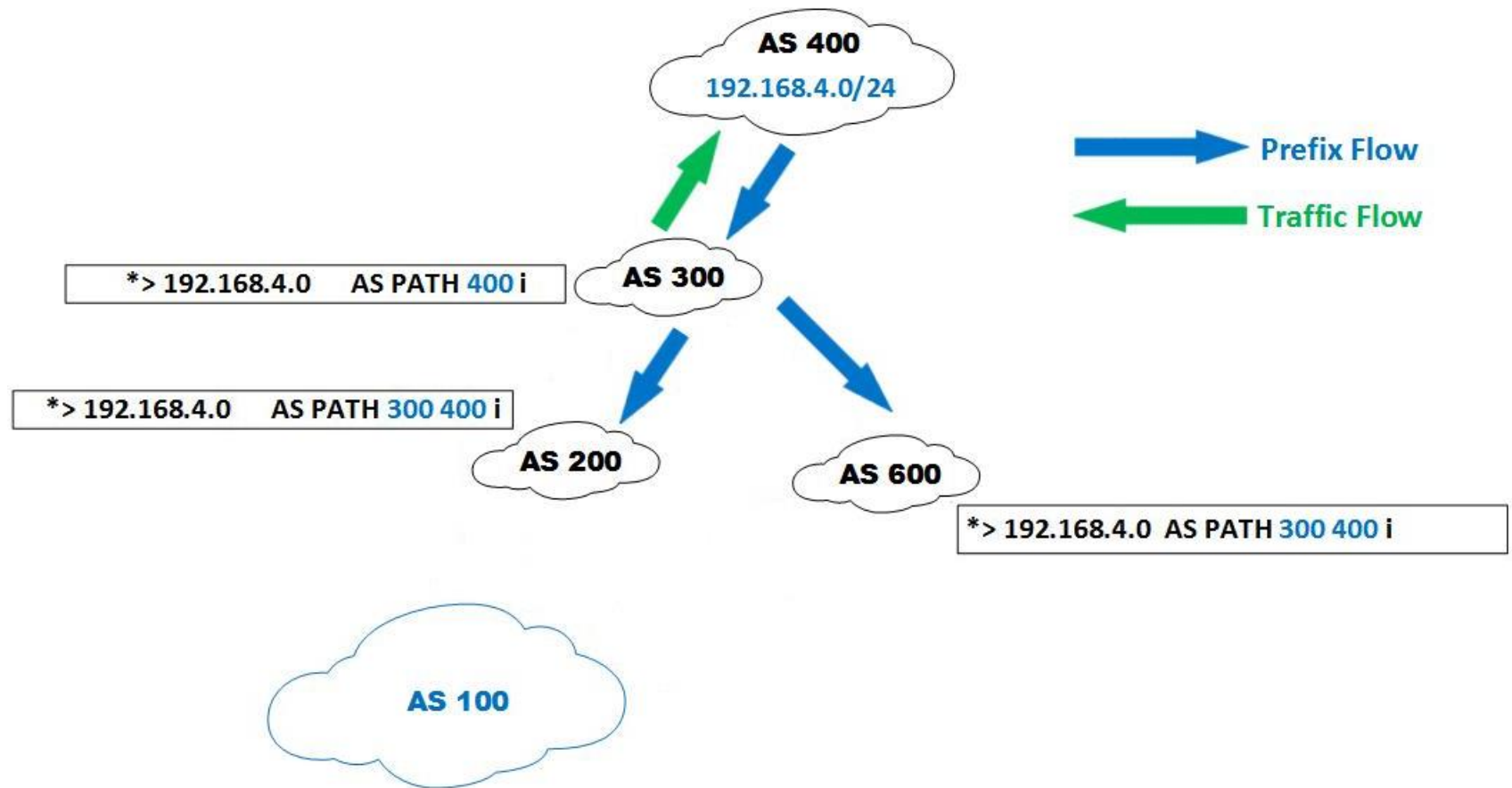
Internet Routing Security

Route Leaks



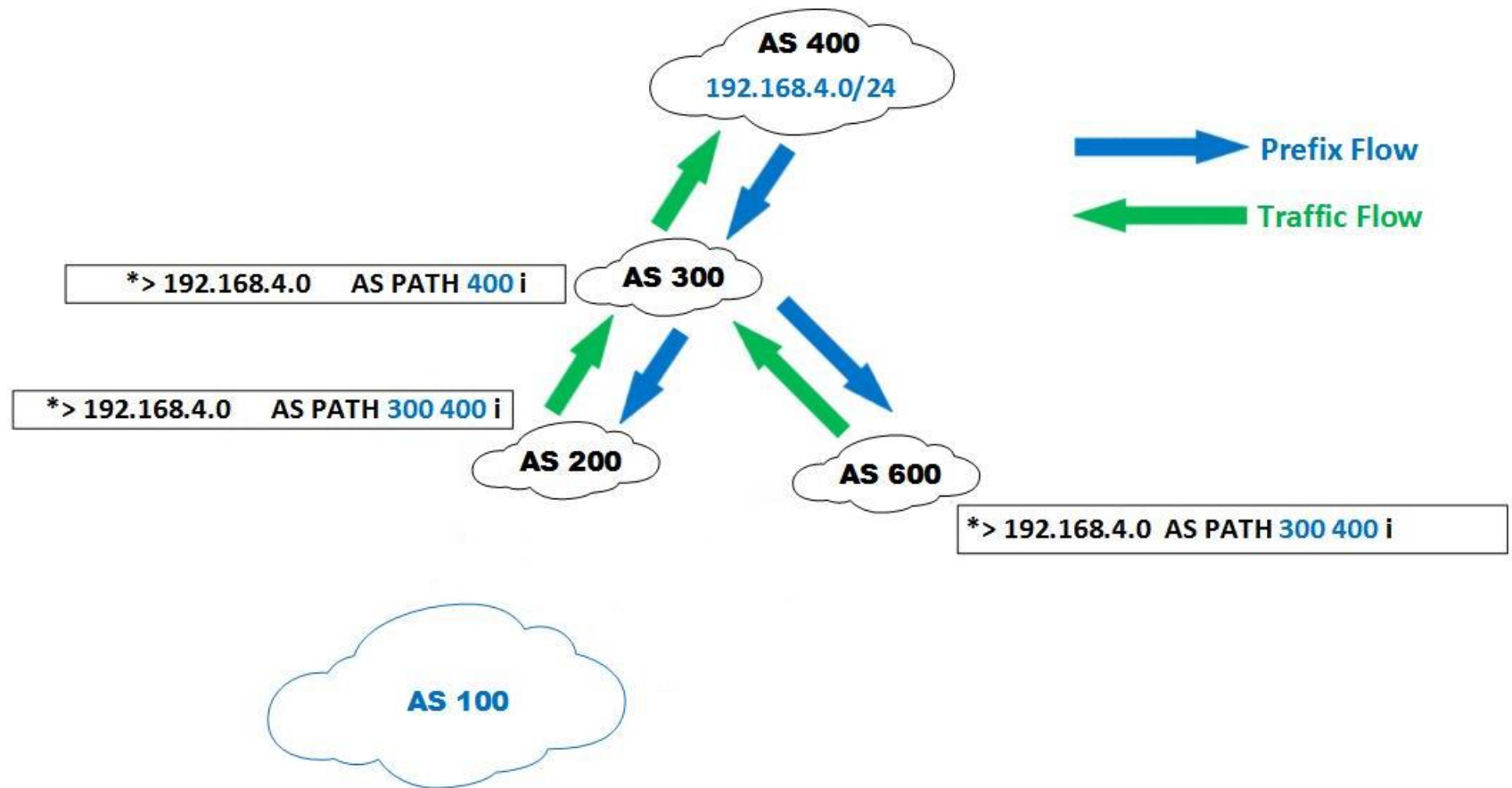
Internet Routing Security

Route Leaks



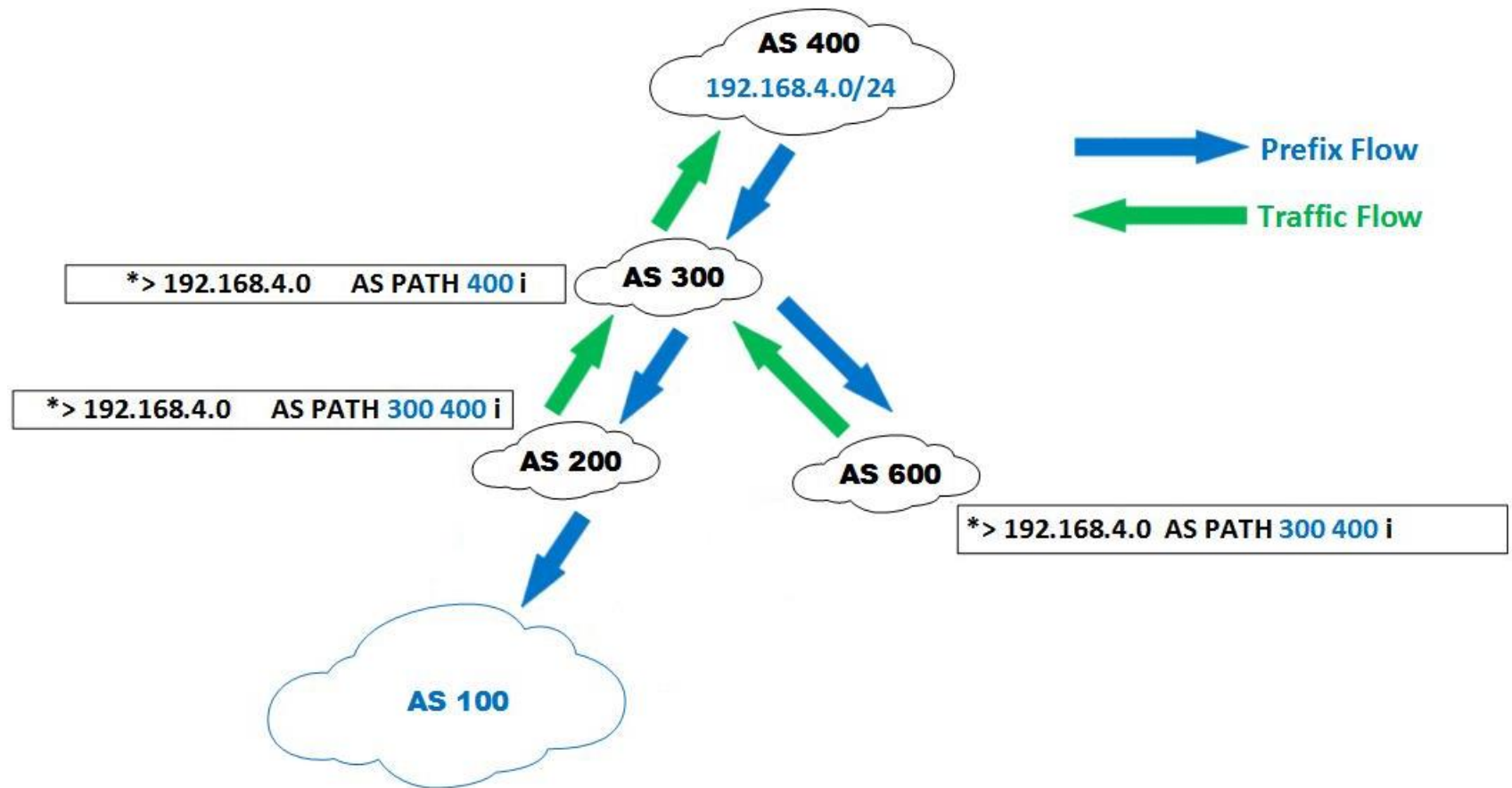
Internet Routing Security

Route Leaks



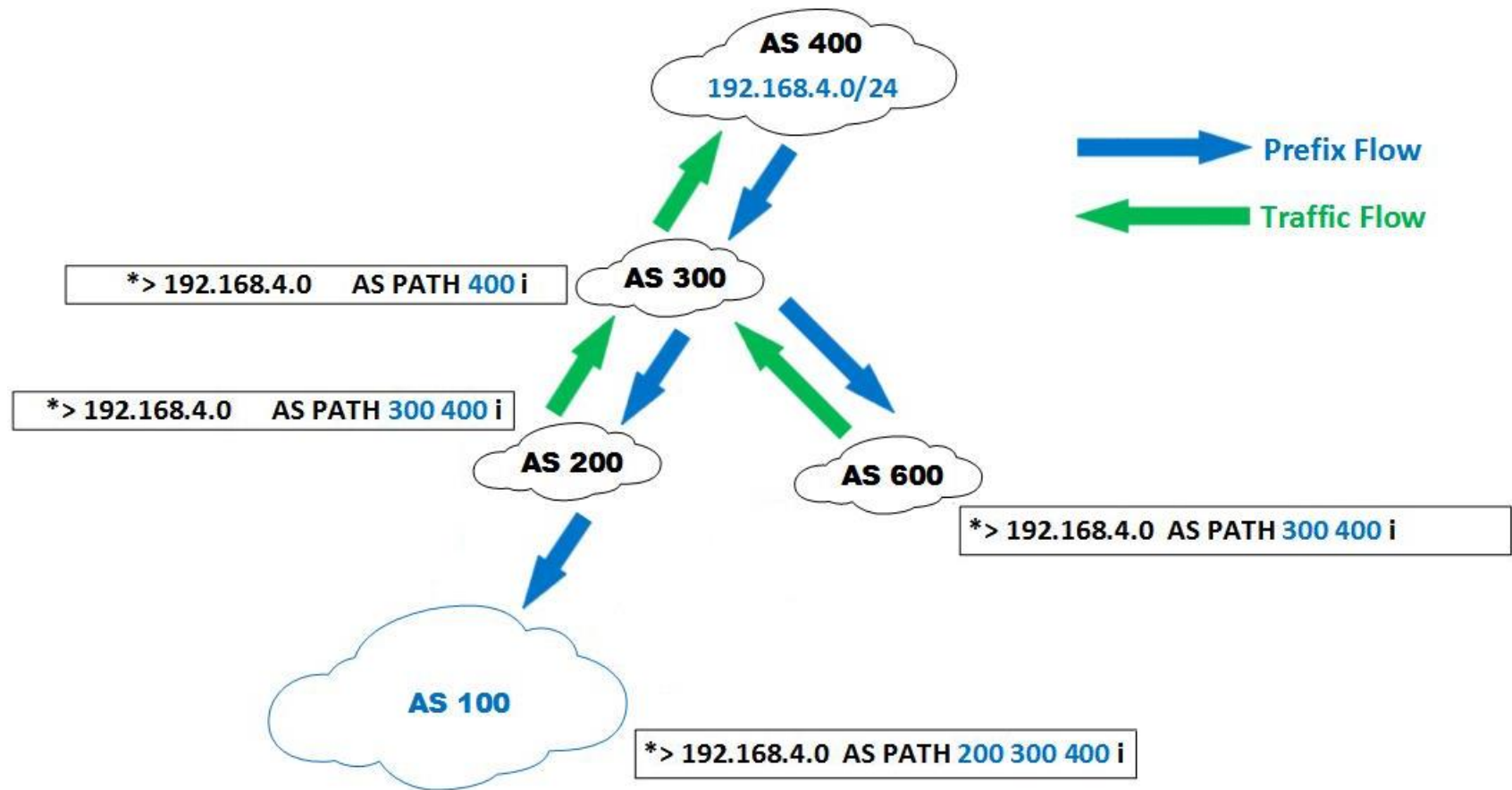
Internet Routing Security

Route Leaks



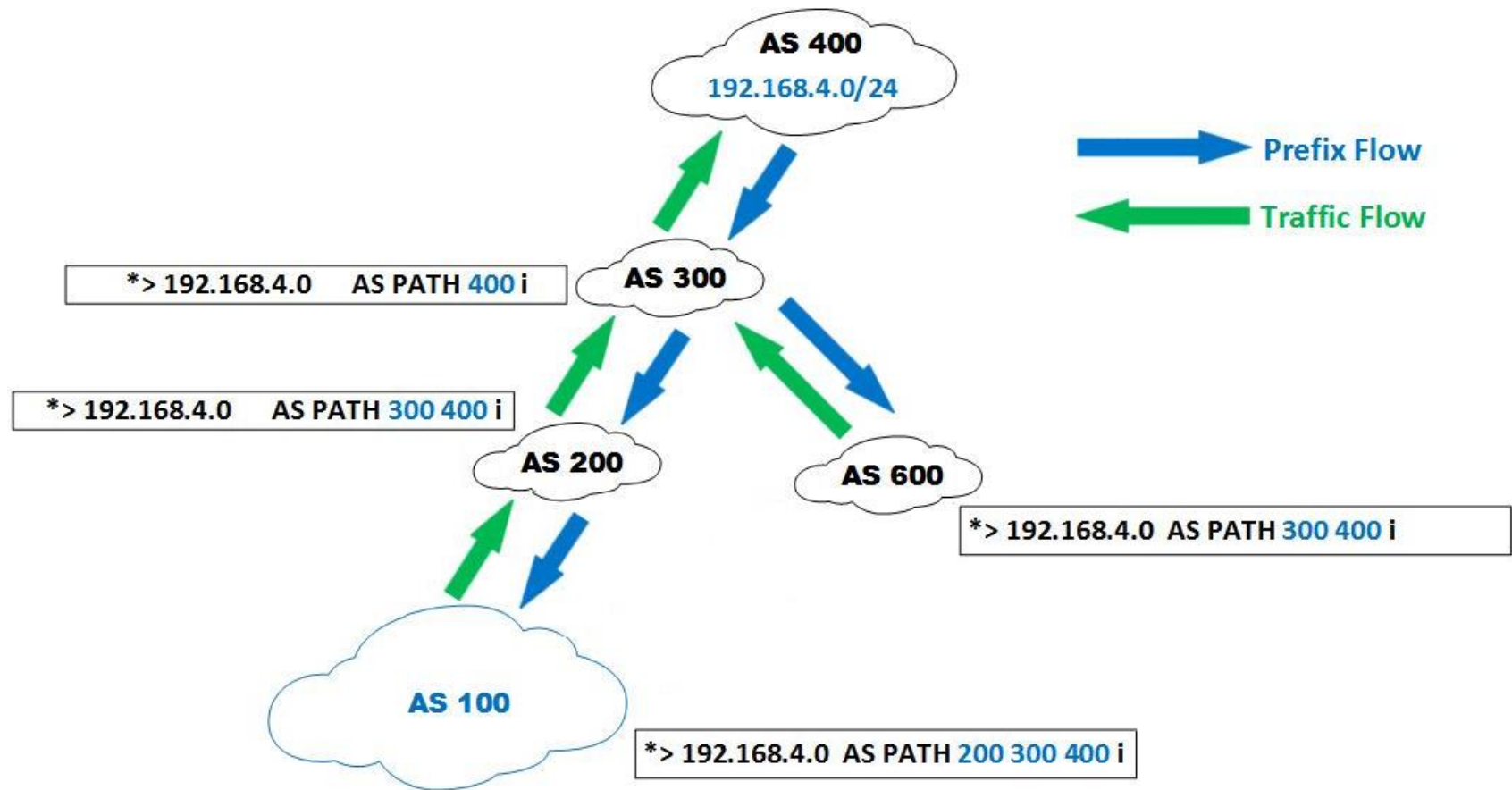
Internet Routing Security

Route Leaks



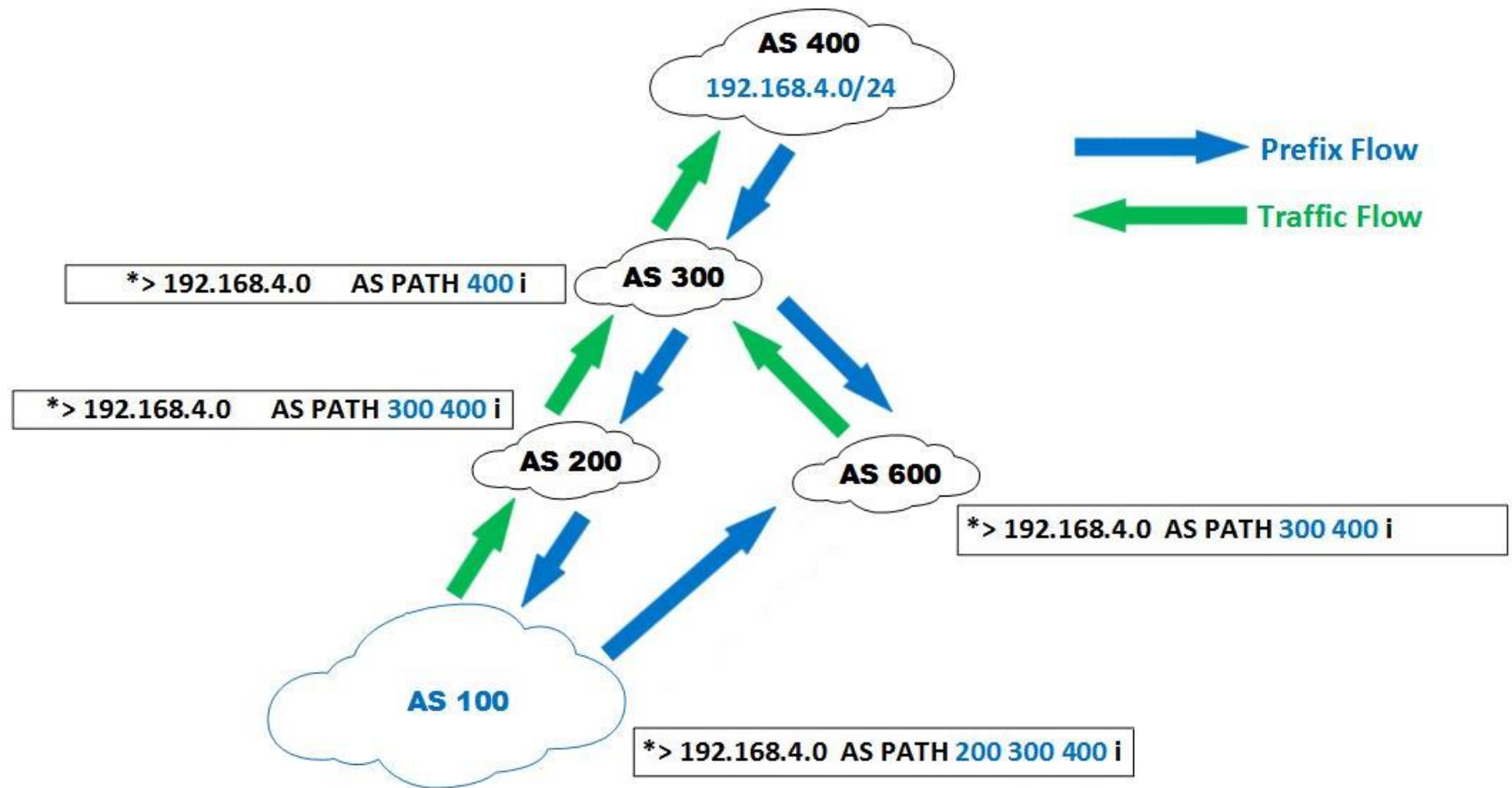
Internet Routing Security

Route Leaks



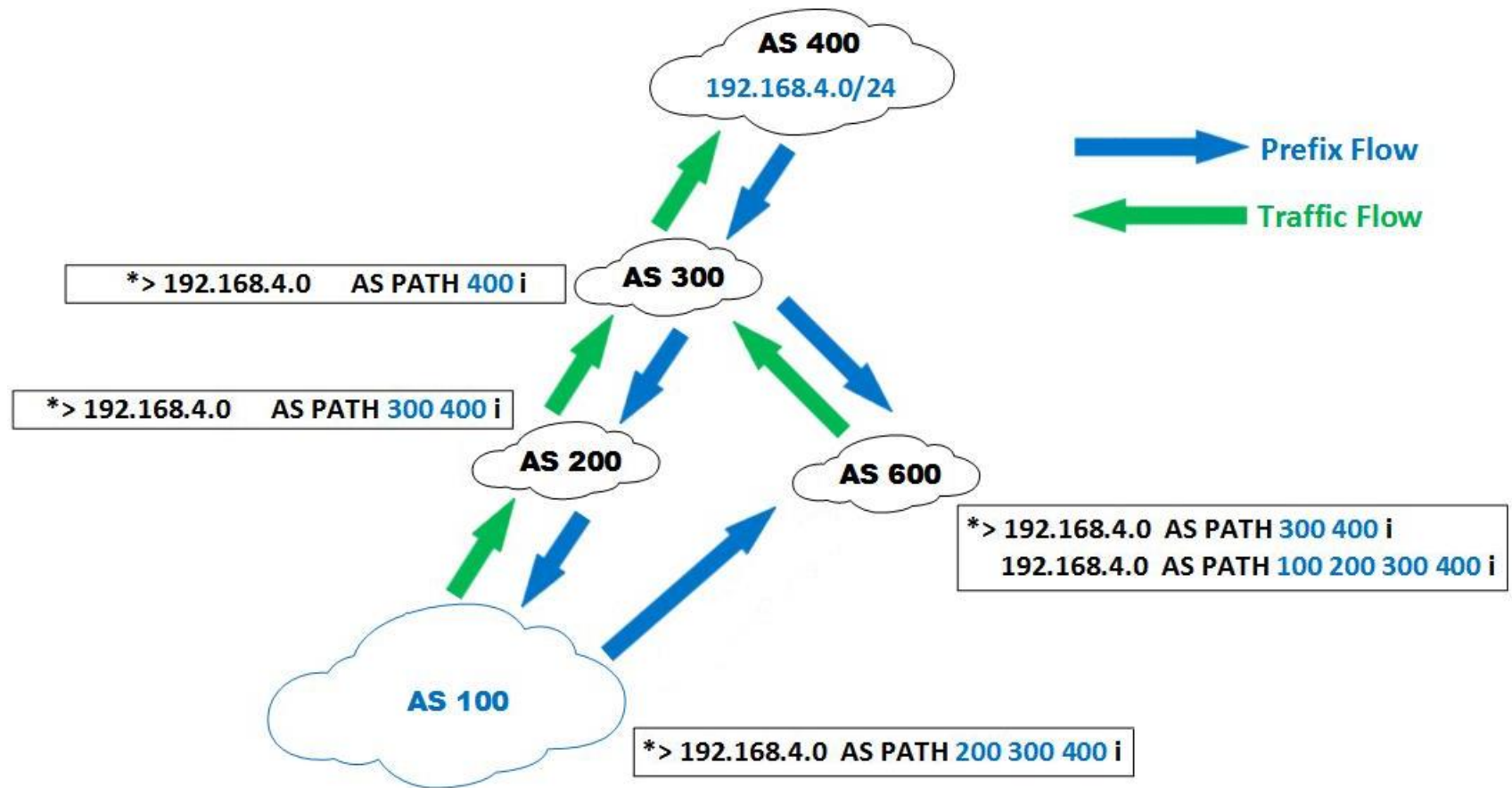
Internet Routing Security

Route Leaks



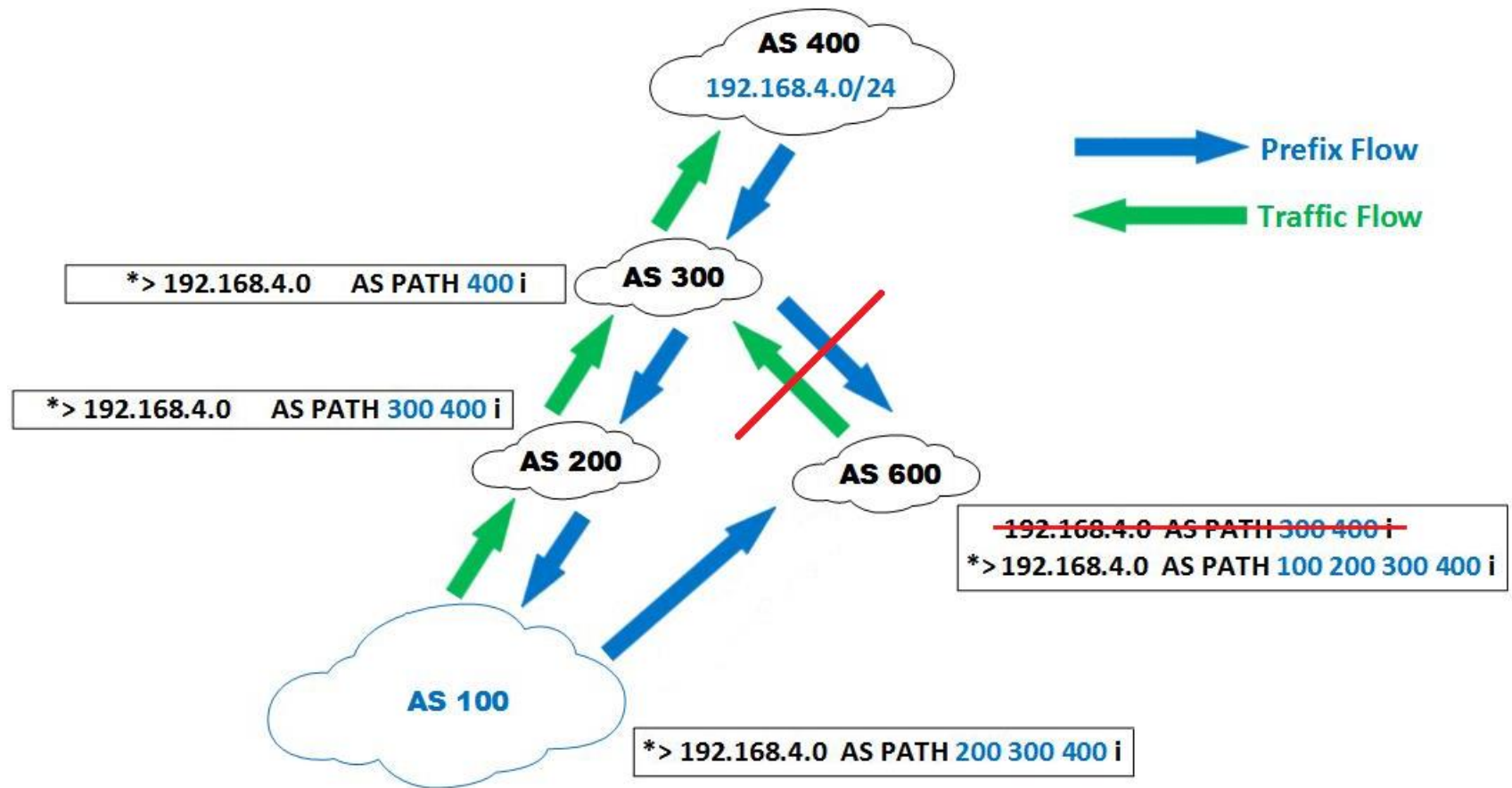
Internet Routing Security

Route Leaks



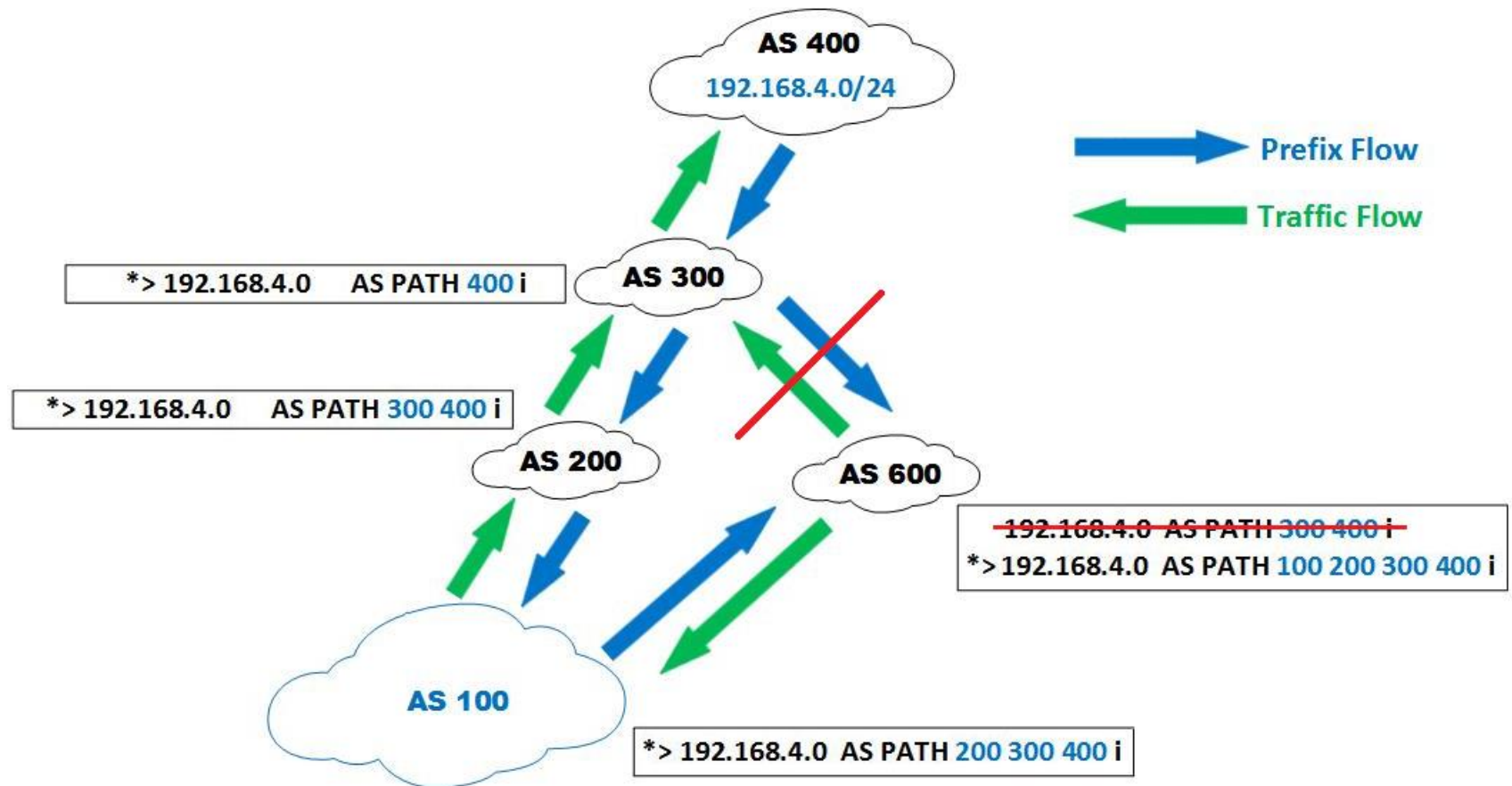
Internet Routing Security

Route Leaks



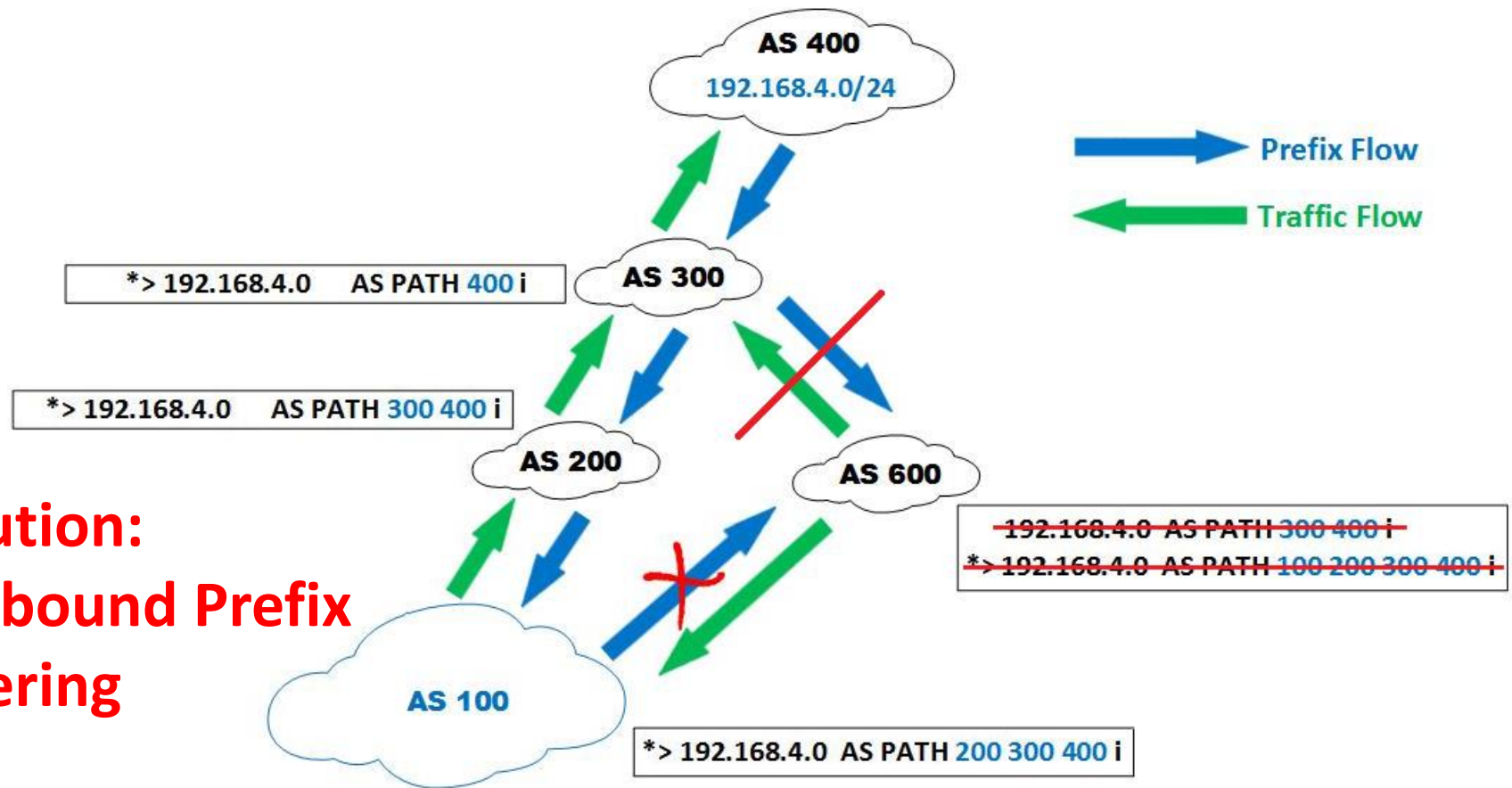
Internet Routing Security

Route Leaks



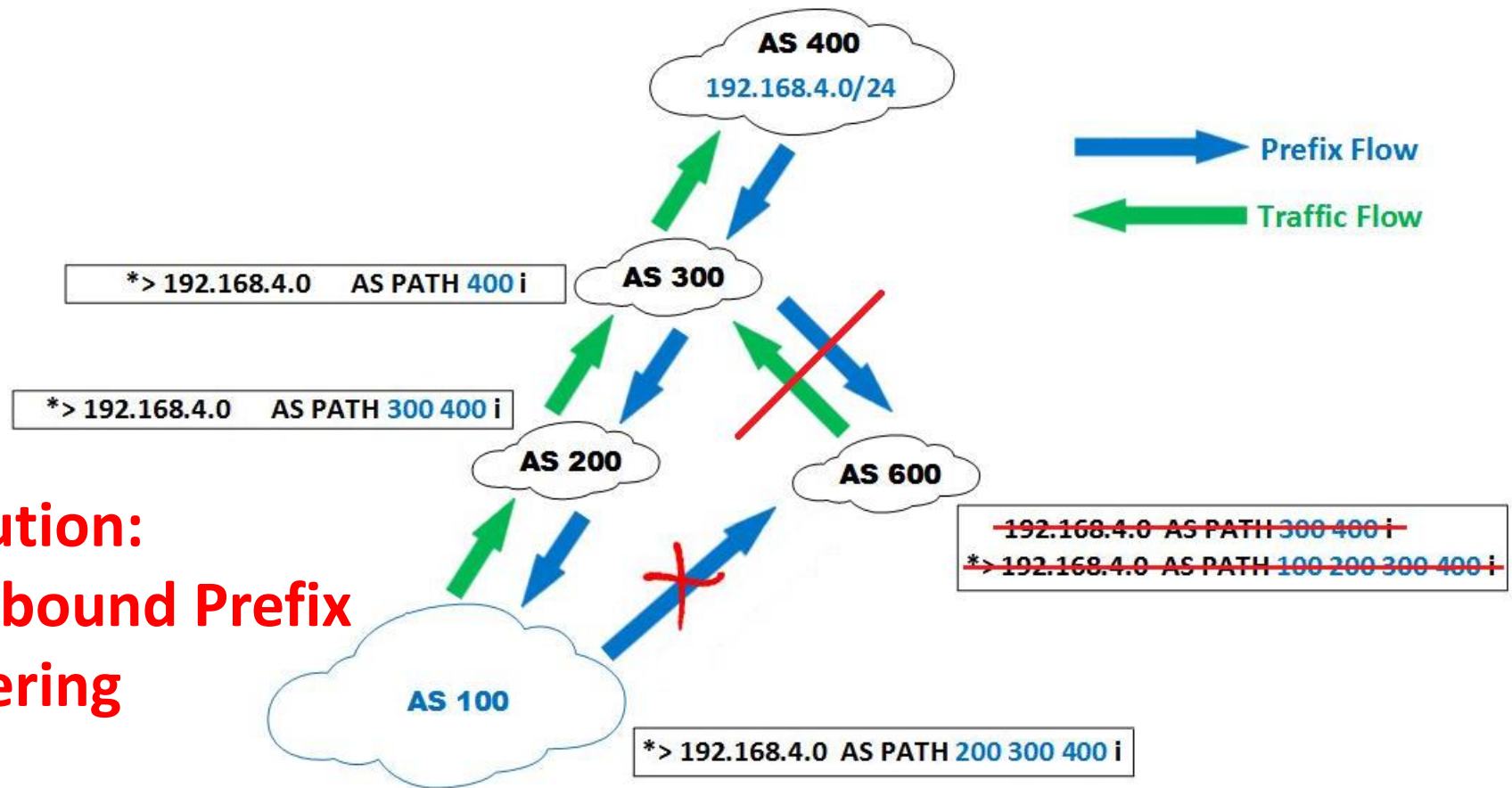
Internet Routing Security

Route Leaks



Internet Routing Security

Route Leaks



Solution:
Outbound Prefix
Filtering

Internet Routing Security

Control Plane vs Data Plane Security

Control Plane

- Prefix filtering can protect your BGP Table/control plane
- **ROA/RPKI** can also be used to protect control plane

Data Plane

- But what about if anyone sends packets with spoofed source IP address?
- **Source address validation** should be there to deal with that!!

Internet Routing Security

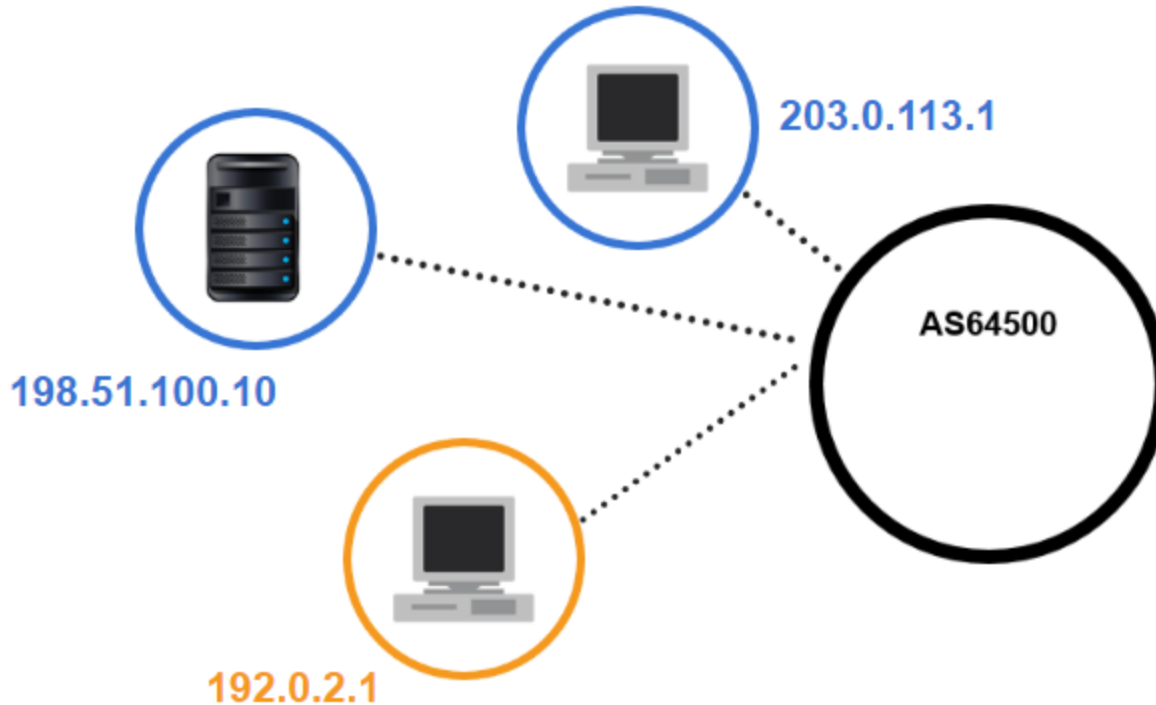
IP Address Spoofing

- IP source address spoofing is the practice of originating IP datagrams with source addresses other than those assigned to the host of origin
- Put simply, the host pretends to be some other host
- Normally when your router receives unicast IP packets it only cares about one thing:

What is the destination IP address of this IP packet so I can forward it?

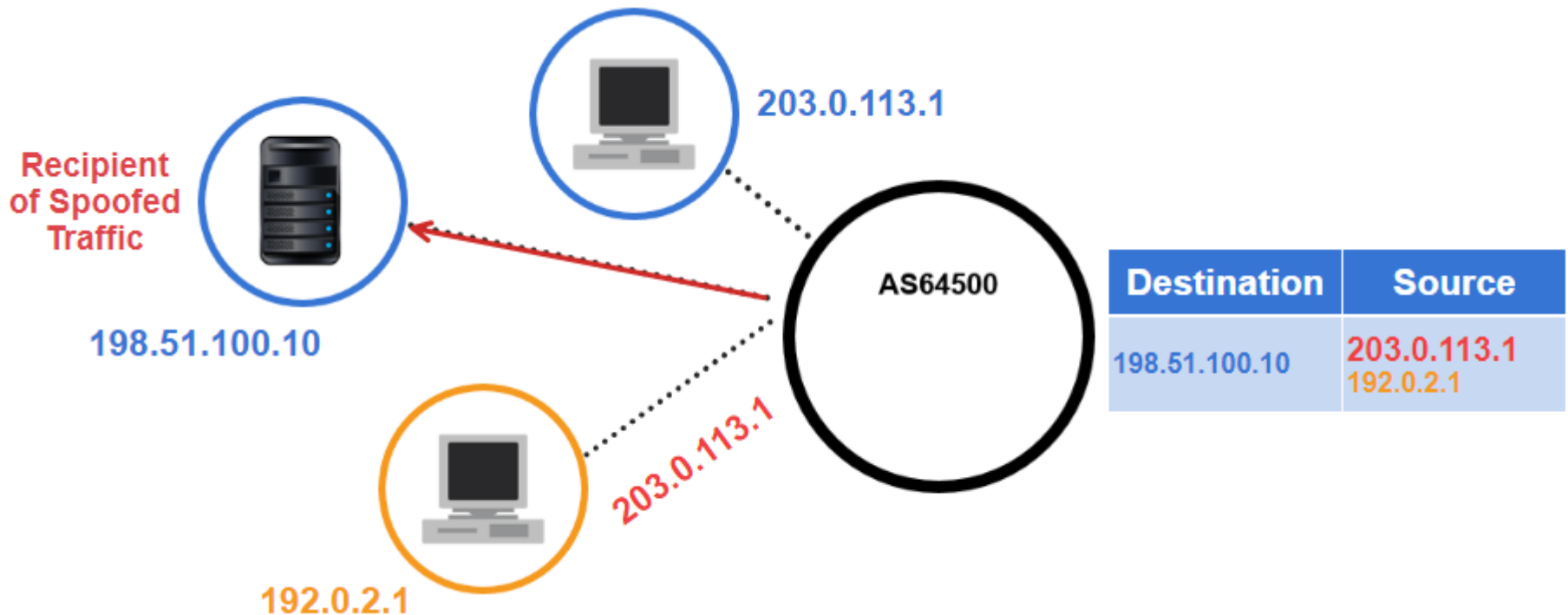
Internet Routing Security

IP Address Spoofing



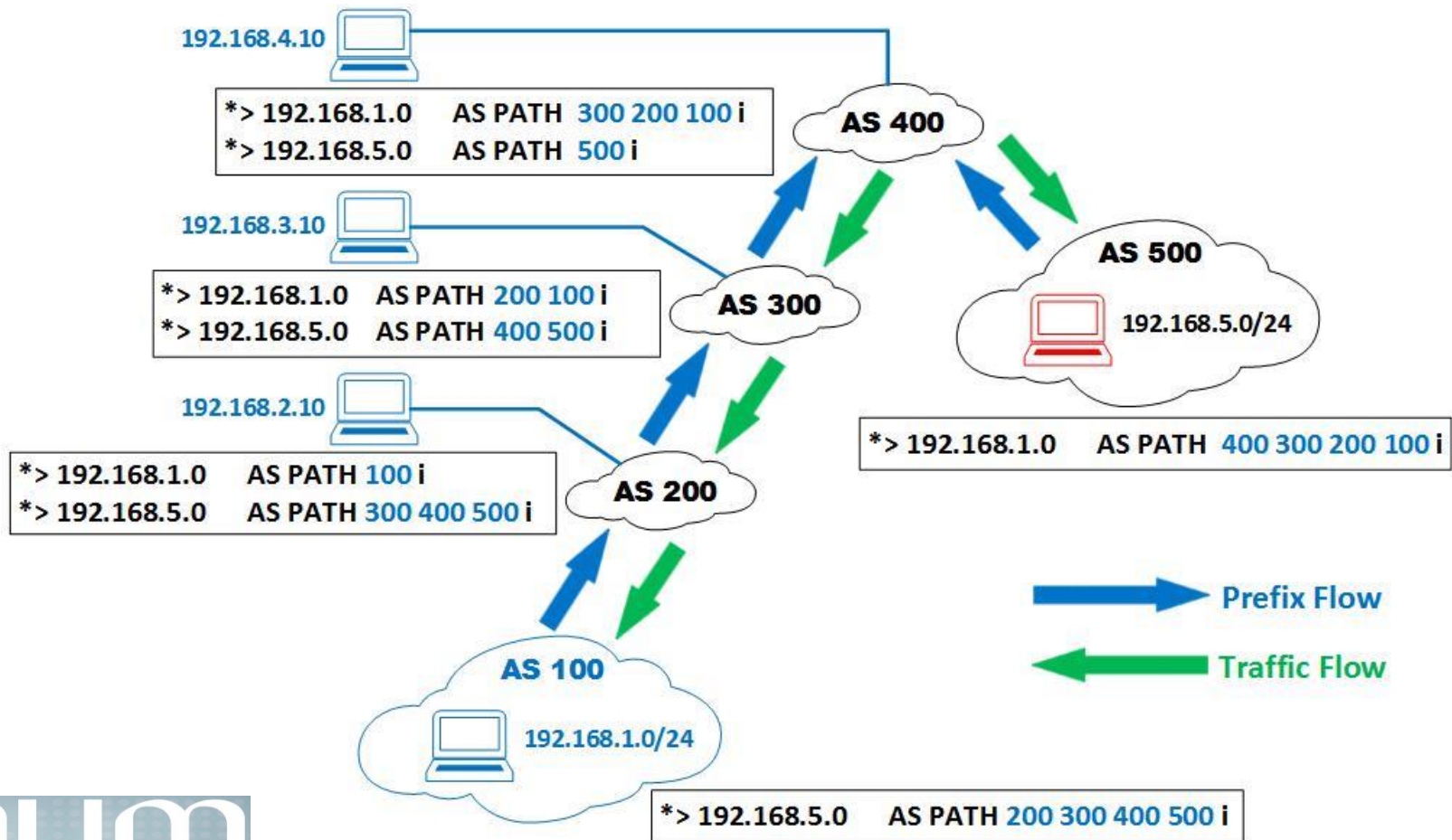
Internet Routing Security

IP Address Spoofing



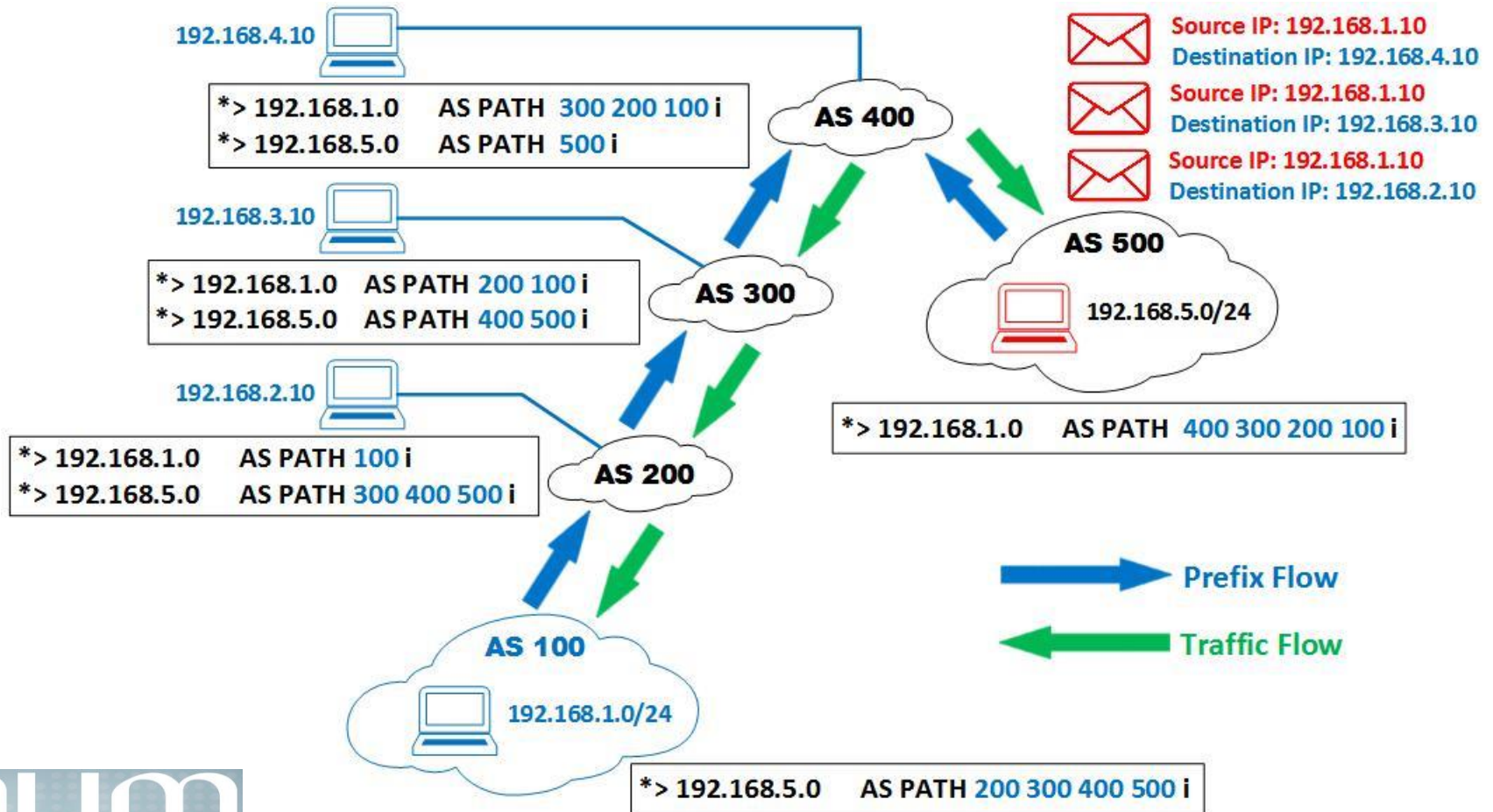
Internet Routing Security

IP Address Spoofing (Sample Attack)



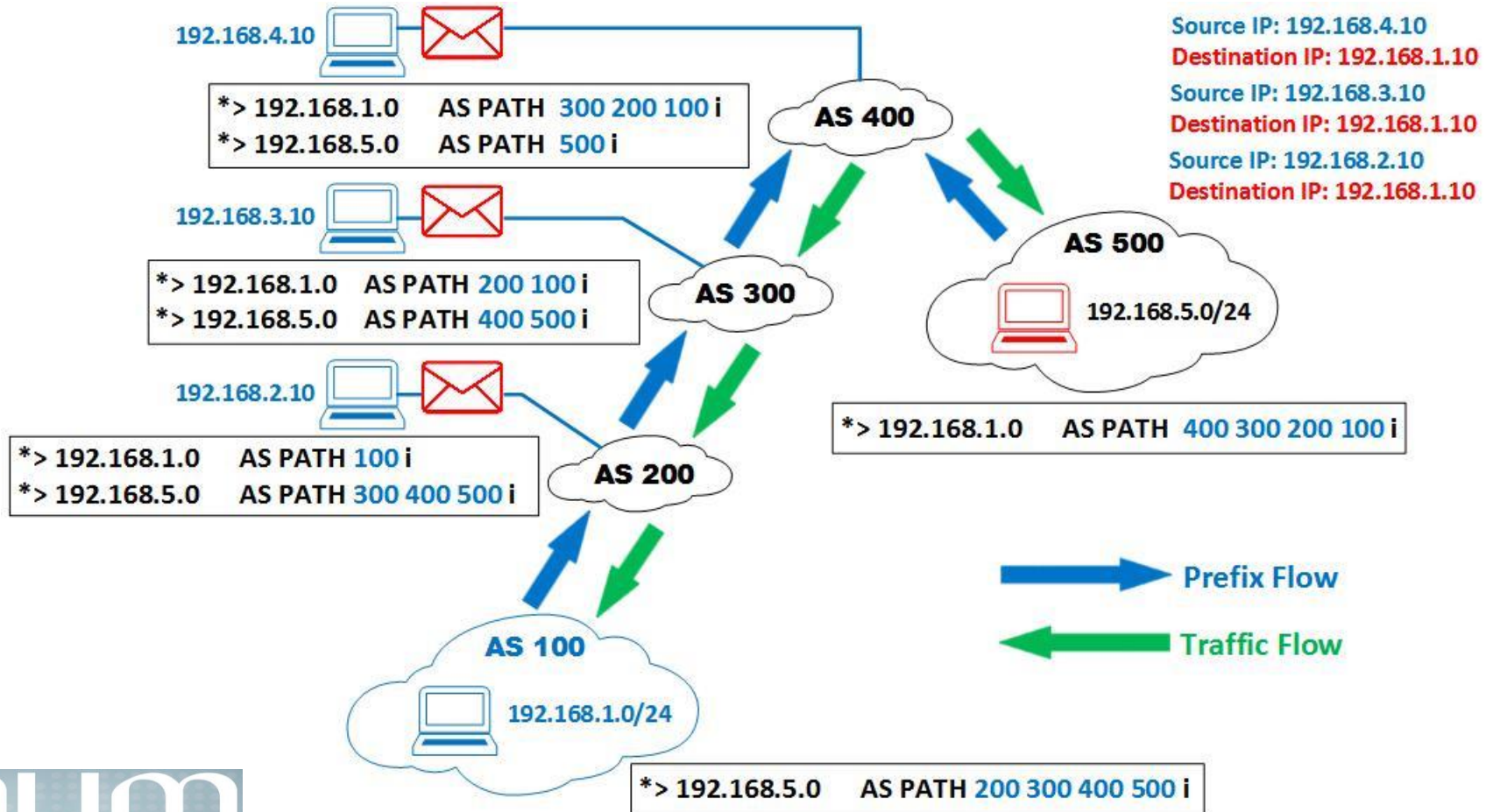
Internet Routing Security

IP Address Spoofing (Sample Attack)



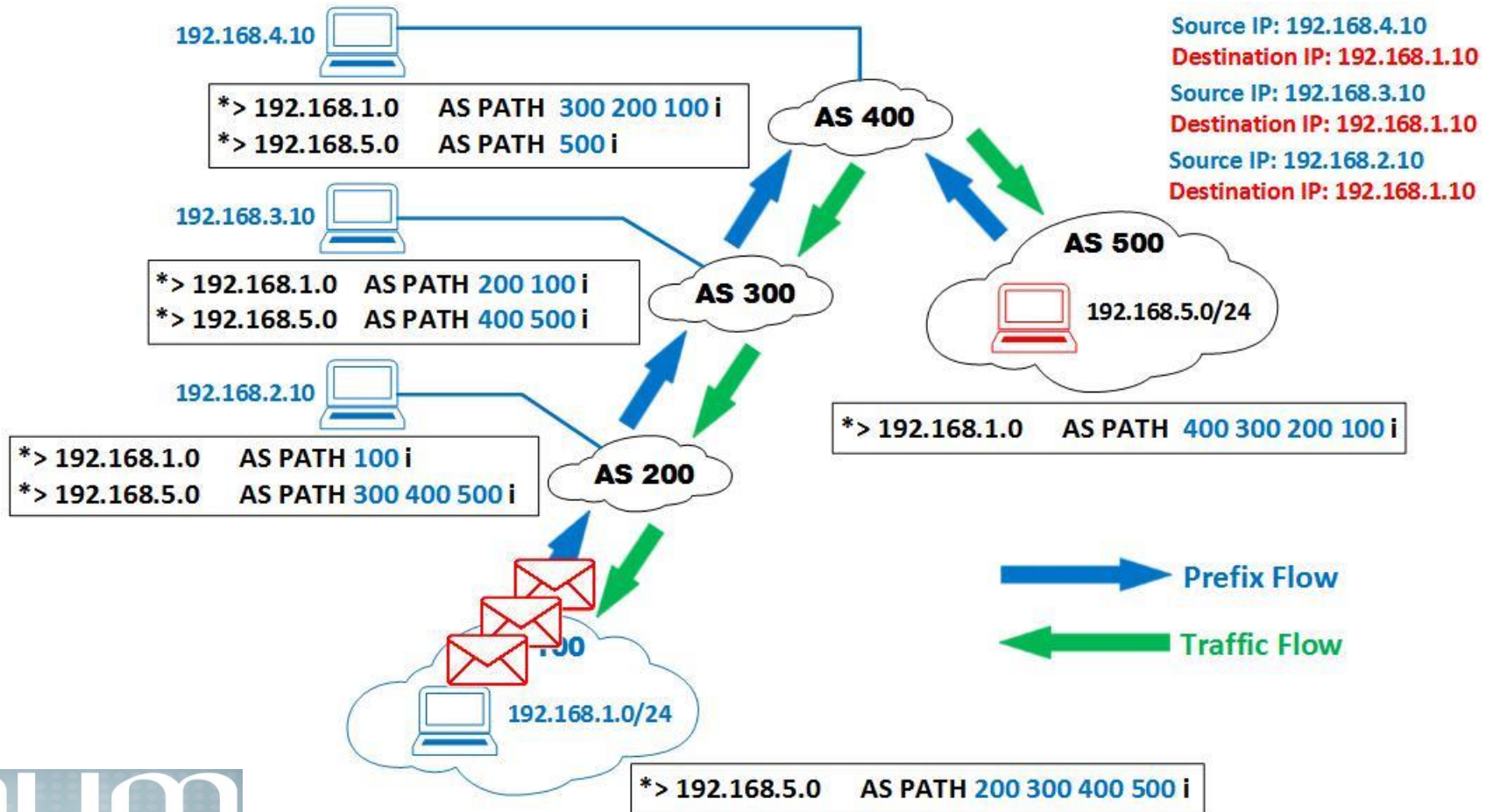
Internet Routing Security

IP Address Spoofing (Sample Attack)



Internet Routing Security

IP Address Spoofing (Sample Attack)



Internet Routing Security

IP Address Spoofing Implications

Spoofing can be exploited in various ways, most notably to execute a DDoS Reflection-Amplification attack



Internet Routing Security

IP Address Spoofing Implications

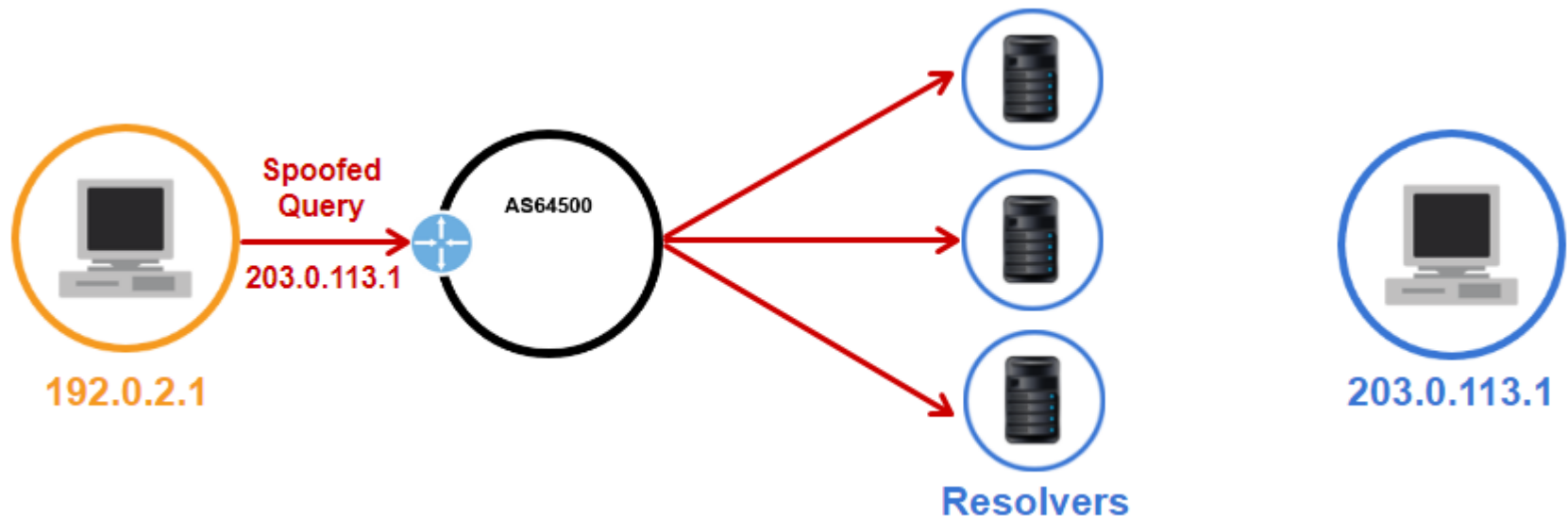
Spoofing can be exploited in various ways, most notably to execute a DDoS Reflection-Amplification attack



Internet Routing Security

IP Address Spoofing Implications

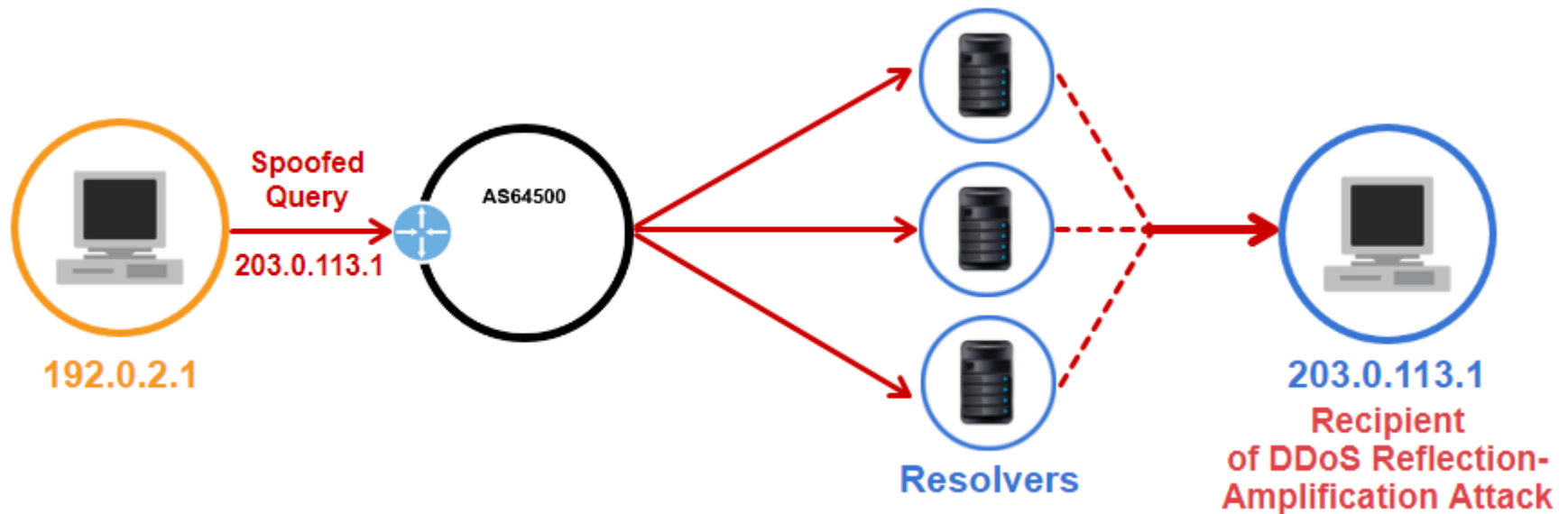
Spoofing can be exploited in various ways, most notably to execute a DDoS Reflection-Amplification attack



Internet Routing Security

IP Address Spoofing Implications

Spoofing can be exploited in various ways, most notably to execute a DDoS Reflection-Amplification attack



Internet Routing Security

IP Address Spoofing Implications

- DDoS Amplification is achieved by small queries resulting in much larger responses
- Open DNS resolvers, NTP servers and Memcache are commonly used as reflectors/amplifiers
- IP Spoofing can be more destructive if a valid **TCP session is hijacked**

Internet Routing Security

IP Address Spoofing Implications

- Significant DoS attacks are costing Service Providers
- These costs hurt the brand, damage customer operations, and have collateral operational/cost impact on other customers

Internet Service Providers in Mumbai targeted in DDoS attack

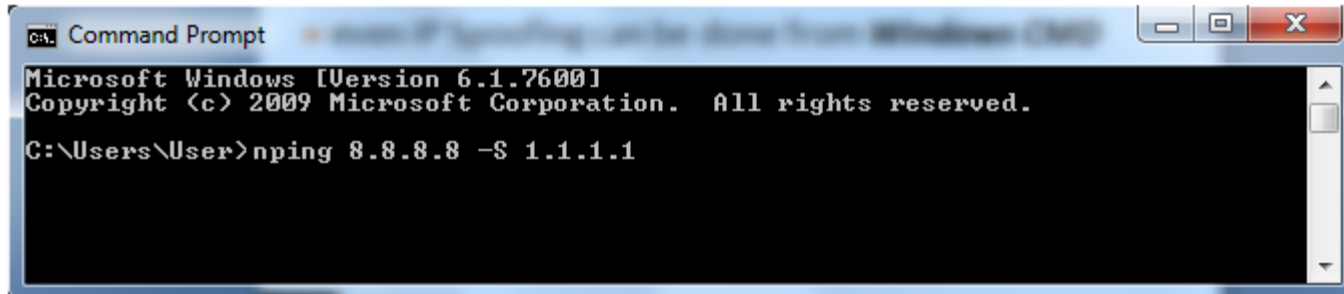
Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Blizzard Entertainment Hit By Multiple DoS Attacks in August 2016

Spoofing Tools

Spoofing Tools

- **nping** (available in *Zenmap* and other tools)
- **synner**
- **kali linux** (popular to *pen testers*)
- even IP Spoofing can be done from ***Windows CMD***



```
Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>nping 8.8.8.8 -S 1.1.1.1
```

Anti-Spoofing

Anti-Spoofing

- DDoS Reflection-Amplification attacks would be **impossible without spoofing** – however, they are preventable
- Implementing anti-spoofing filtering to **prevent packets with incorrect source IP address** from entering the network

Anti-Spoofing

Anti-Spoofing Techniques

- Ingress Packet Filtering
- unicast Reverse Path Forwarding



Packet Filtering



uRPF

Anti-Spoofing

Anti-Spoofing Techniques Considerations

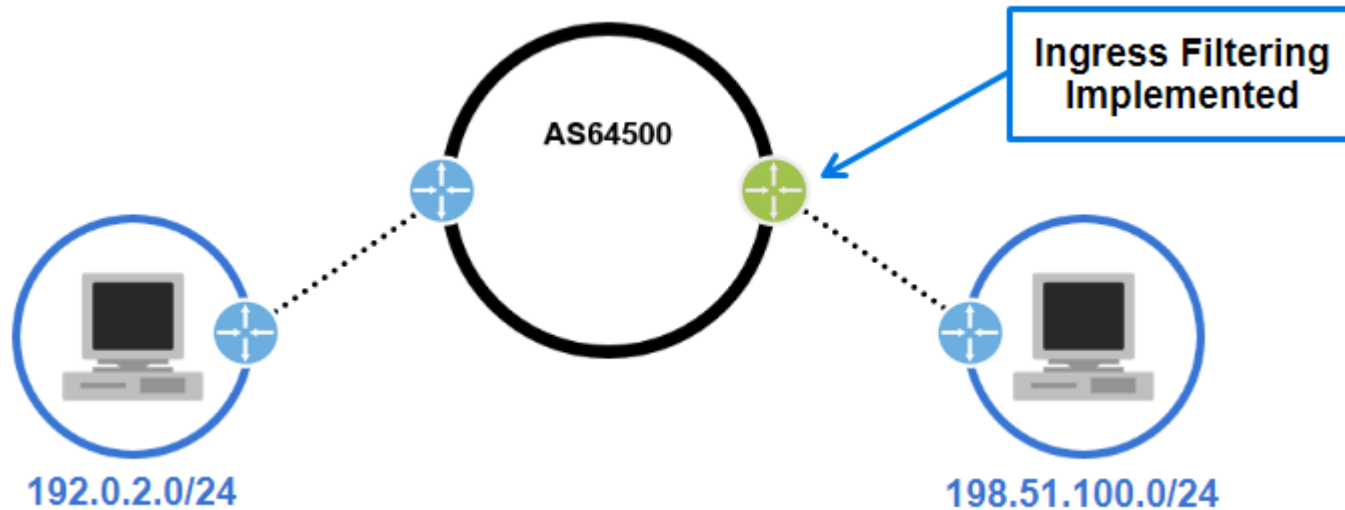
- Identify points/devices in the network topology where anti-spoofing measures should be applied
- Identify adequate techniques to be used (for example, uRPF, or filtering)
- Apply configuration commands
- Verify that the protection works

Anti-Spoofing

Anti-Spoofing Techniques

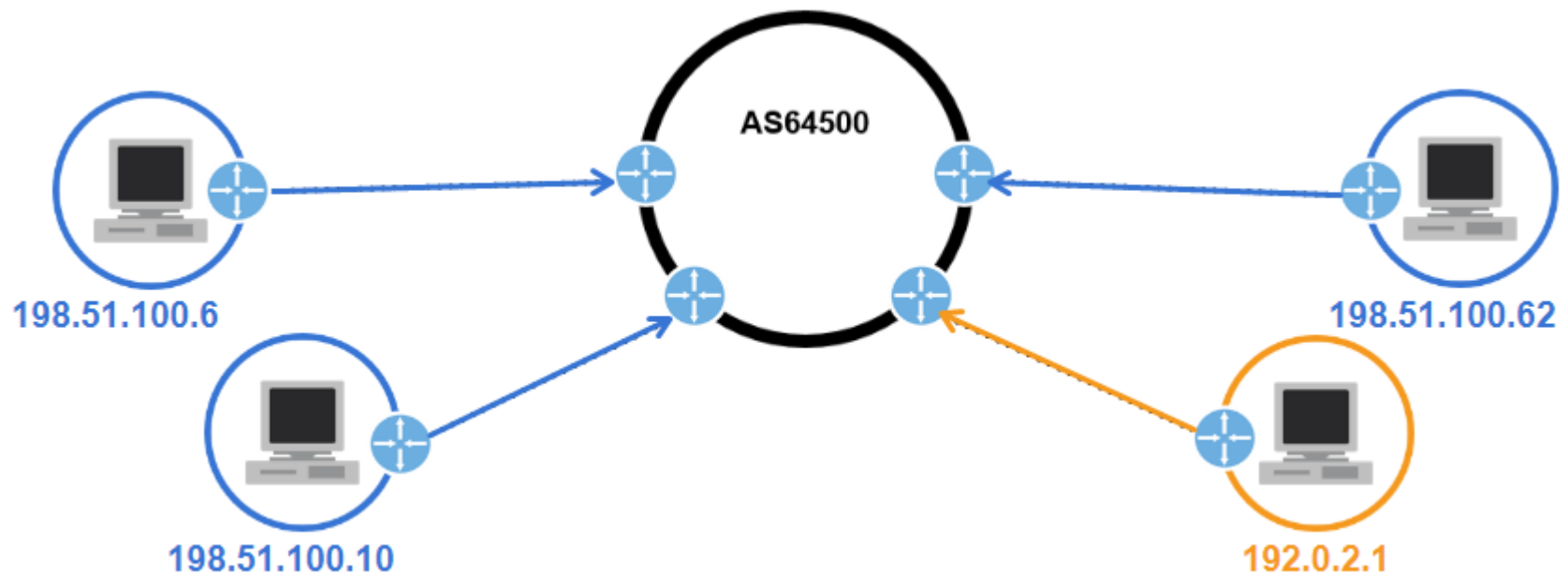
To prevent source IP address spoofing, it's recommended to implement **Ingress Filtering** methods which include:

Ingress Filtering, uRPF etc



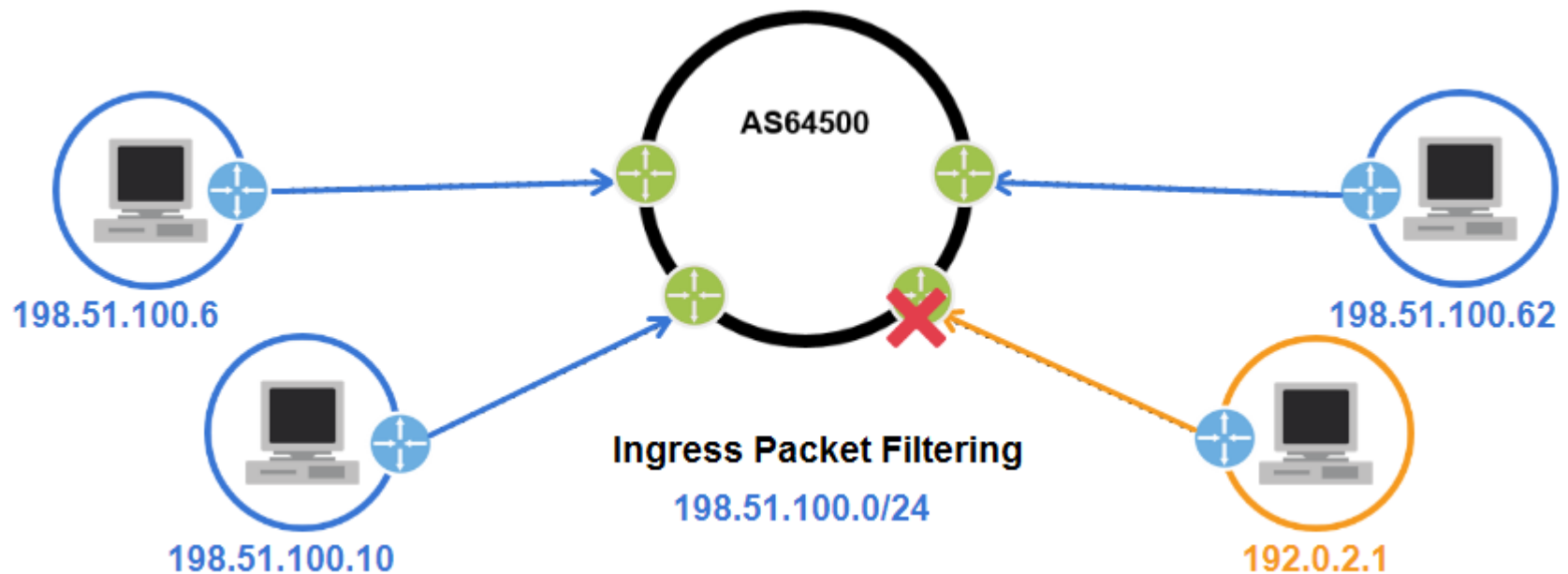
Anti-Spoofing

Anti-Spoofing Techniques - Ingress Packet Filtering



Anti-Spoofing

Anti-Spoofing Techniques - Ingress Packet Filtering



Anti-Spoofing

Anti-Spoofing Techniques - Ingress Packet Filtering

```
/ip firewall filter add action=drop chain=forward \  
comment="spoofed from AS64501"\  
in-interface=$interface log-prefix=""\  
src-address=!192.0.2.0/24
```



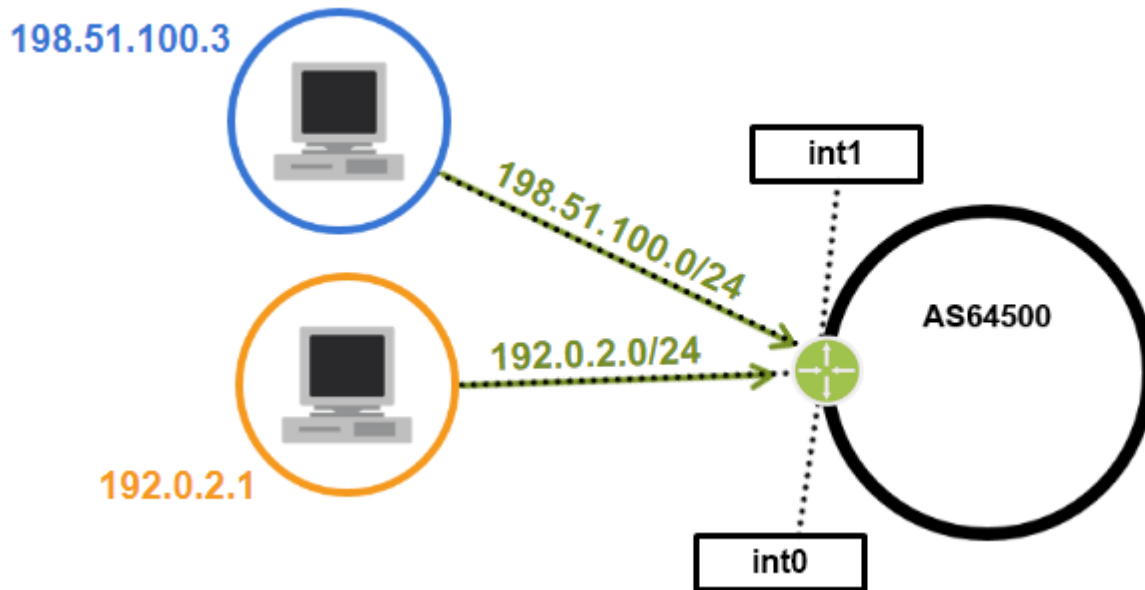
```
/ipv6 firewall filter add action=drop chain=forward\  
comment="spoofed from AS64501"\  
in-interface=$interface log-prefix=""\  
src-address=!2001:db8:1001::/48
```

Anti-Spoofing Techniques - uRPF

- uRPF is a security feature that prevents these spoofing attacks. Whenever your router receives an IP packet it will check if it has a **matching entry in the routing table for the source IP address**. If it doesn't match, the packet will be discarded
- uRPF as defined in **RFC 3704**
- uRPF is often implemented on the edges of the networks where customers, servers, and/or clients are connected

uRPF

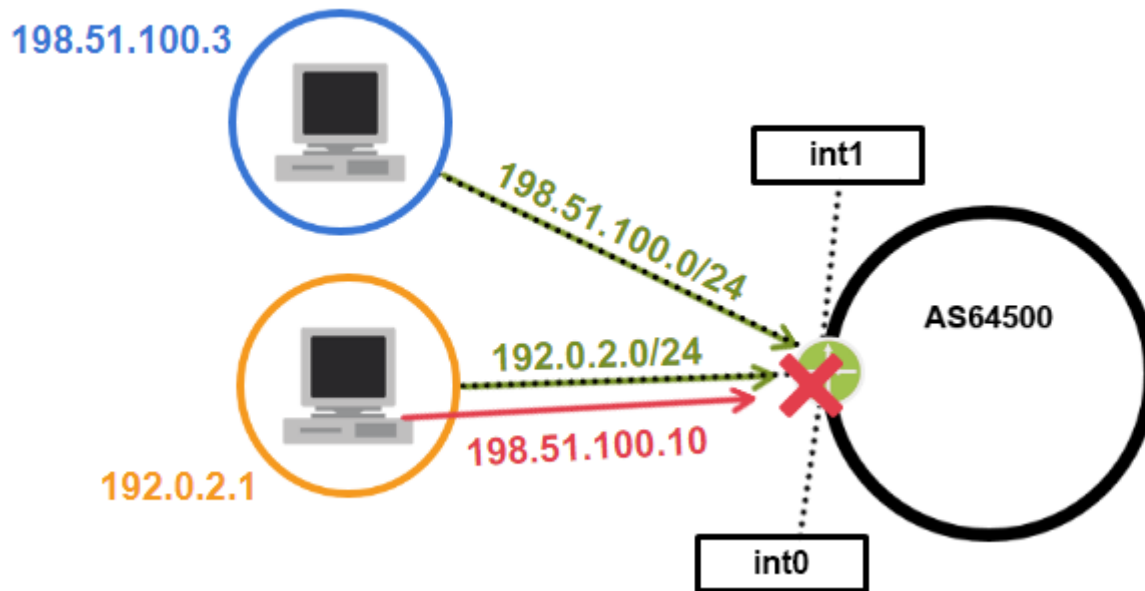
Anti-Spoofing Techniques - uRPF



FIB	
198.51.100.0/24	int1
192.0.2.0/24	int0

uRPF

Anti-Spoofing Techniques - uRPF



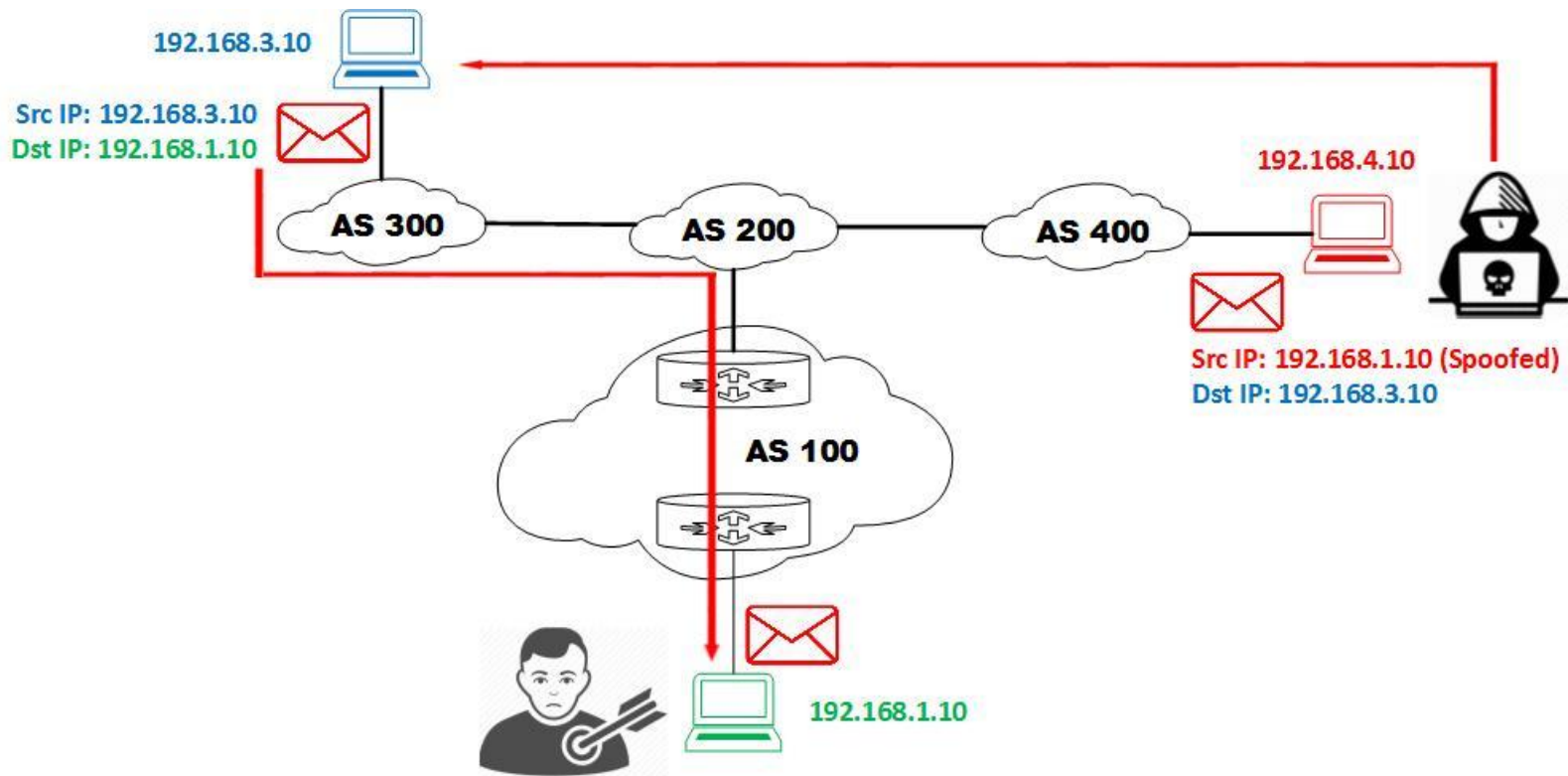
FIB	
198.51.100.0/24	int1
192.0.2.0/24	int0

Announced network	Incoming pkt source ip
192.0.2.0/24	198.51.100.10 192.0.2.1

A FIB record for 198.51.100.10 does not correspond to the incoming interface.

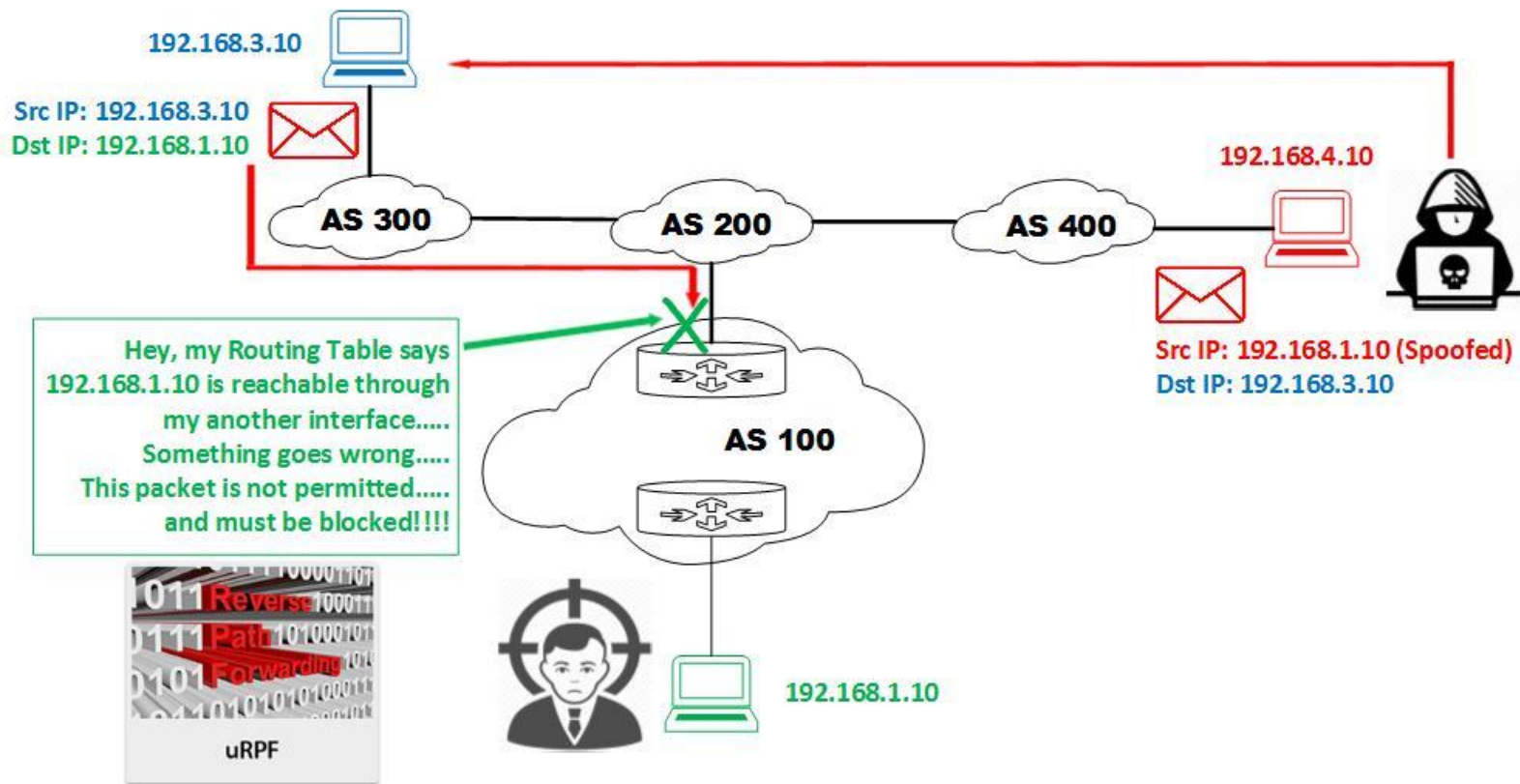
uRPF

Anti-Spoofing Techniques - uRPF



uRPF

Anti-Spoofing Techniques - uRPF



uRPF

There are four modes for uRPF:

- **Loose Mode**
- **Strict Mode**
- **Feasible Mode**
- **VRF Mode**

MikroTik supports *Loose Mode* and *Strict Mode*

- For **single-homed stub customers**, it's recommended that **uRPF strict mode** is implemented
- For **dual-homed stub customers**, it is best to use **uRPF feasible** mode instead

uRPF

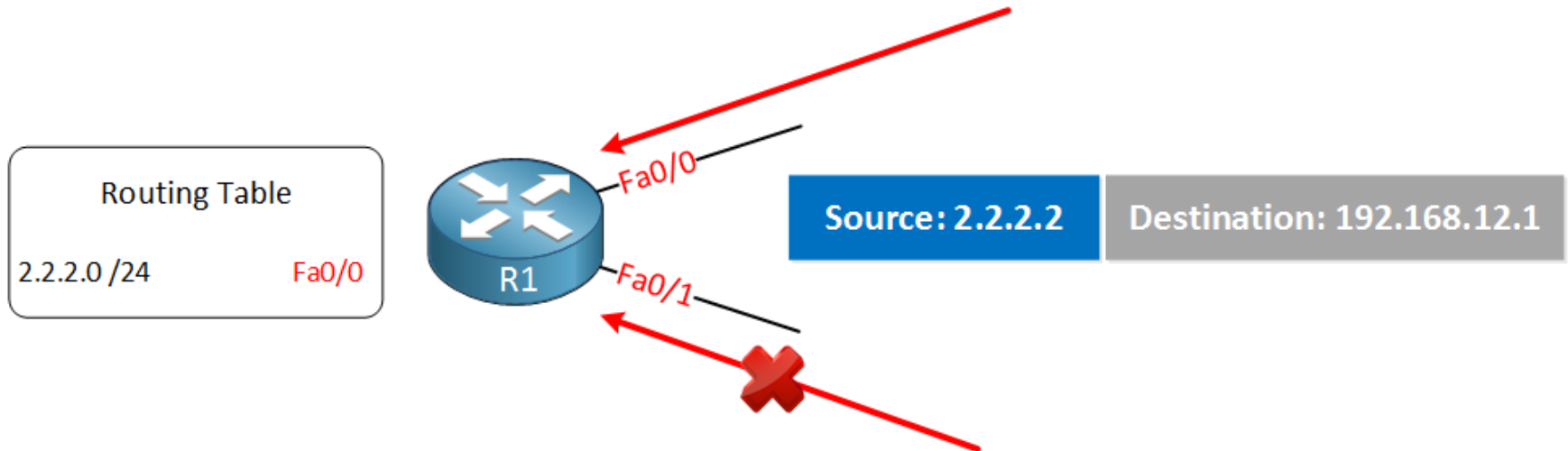
uRPF Strict Mode

In **Strict mode** router will perform **two checks**:

1. Do I have a matching entry for the source in the **routing table**?
2. Do I use the **same interface to reach this source** as where I received this packet on?

uRPF

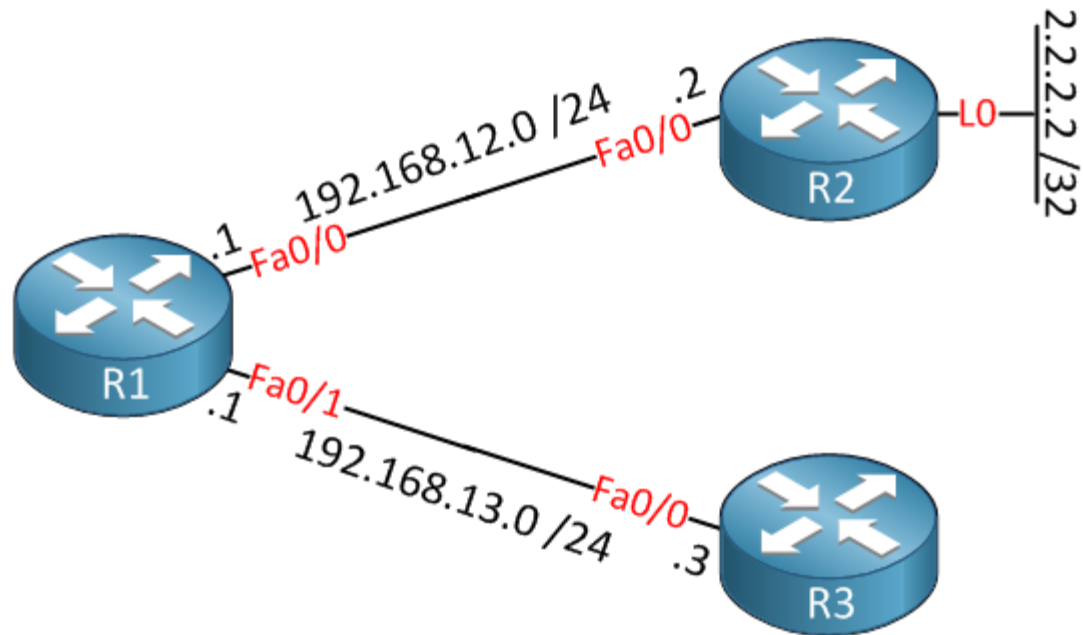
uRPF Strict Mode



When the incoming IP packets **passes both checks**, it will be permitted. Otherwise it will be dropped. This is perfectly fine for IGP routing protocols since they use the shortest path to the source of IP packets.

uRPF

uRPF Strict Mode



uRPF

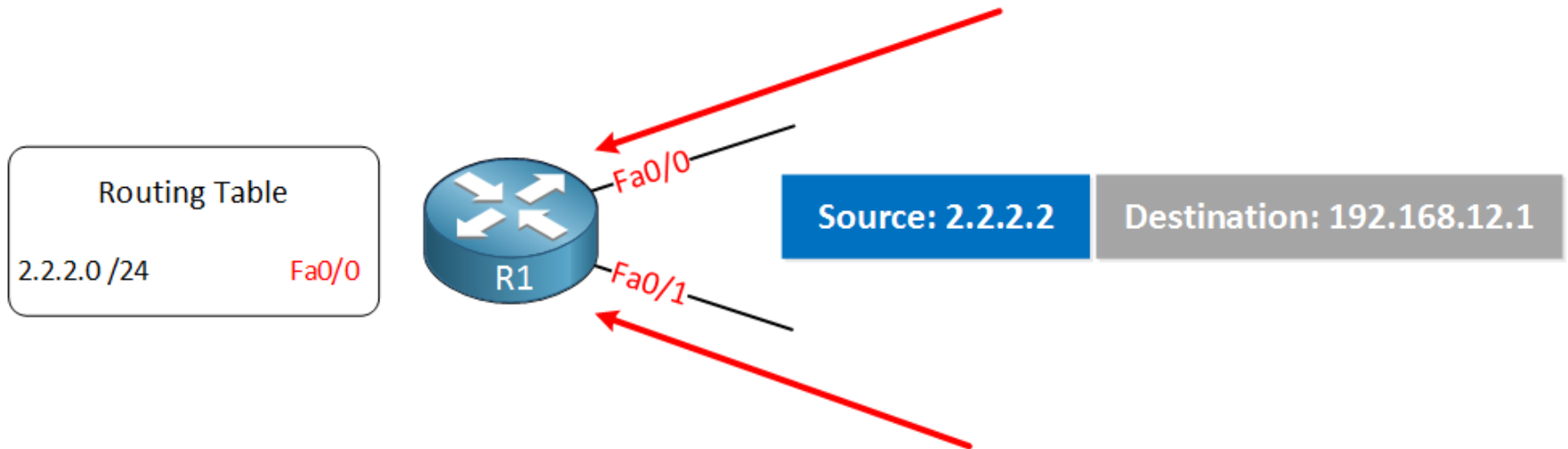
uRPF Loose Mode

In **Loose mode** router will perform only **single check**:

1. Do I have a matching entry for the source in the **routing table**?

uRPF

uRPF Loose Mode



When it passed this check, the packet is permitted. It doesn't matter if we use this interface to reach the source or not. Loose mode is useful when you are connected to more than one ISP and you use **asymmetric routing**.

uRPF

Anti-Spoofing Techniques – uRPF

/ip settings set rp-filter=strict

Or

/ip settings set rp-filter=loose



Recap

To Keep Internet Routing Secure



Recap

Filtering

In order to **prevent propagation of incorrect routing information**, network operators must ensure the correctness of their own announcements, and announcements from their customers to adjacent networks with prefix and AS-path granularity.

Recap

Anti-Spoofing

In order to **prevent traffic with spoofed source IP addresses**, network operators must enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure.

Acknowledgement

- Rene Molenaar
- MANRS
- MikroTik Wiki

Keep Internet Secure 😊



*Mikro***Tik**
Thank You