Routing Security Tool

RoseT

Mariano Scazzariello *, **Antonio Prado** †, Tommaso Caiazzi ‡,

* Research Institutes of Sweden

† "G. D'Annunzio" University, Italy ‡ Roma Tre University, Italy

MANRS Actions For Network Operators

Routing Security Tool
Rose-T

Coordination

Network operators maintain globally accessible up-to-date contact information

Global Validation

Network operators must publicly document their routing policies, ASNs and prefixes

Anti-Spoofing

Prevent packets with spoofed source IP address from entering or leaving the network

Filtering

Prevent propagation of incorrect routing information

MANRS Guidelines For Network Operators

Routing Security Tool
Rose-T

Coordination

Network operators maintain globally accessible up-to-date contact information

Global Validation

Network operators must publicly document their routing policies, ASNs and prefixes

Anti-Spoofing

Prevent packets with spoofed source IP address from entering or leaving the network

Filtering

Prevent propagation of incorrect routing information

How Can a Network Operator Ensure the MANRS Compliance?

How Can a Network Operator Ensure the MANRS Compliance?

Routing Security Tool
Rose-T

Coordination **Global Validation** **Anti-Spoofing** **Filtering**

No suitable tool to automatically verify MANRS compliance!

Operators have to check their configurations and routing policies
manually or with **minimal aid**

Not an easy task!

Not an easy task!

Routing Security Tool
Rose-T

How can we do that?

Simulation?

Good for testing how the network behaves in theory

Cannot consider real configurations and software

Require complex modelling

Not an easy task!

Routing Security Tool
Rose-T

How can we do that?

Simulation?

Good for testing how the network behaves in theory

Cannot consider real configurations and software

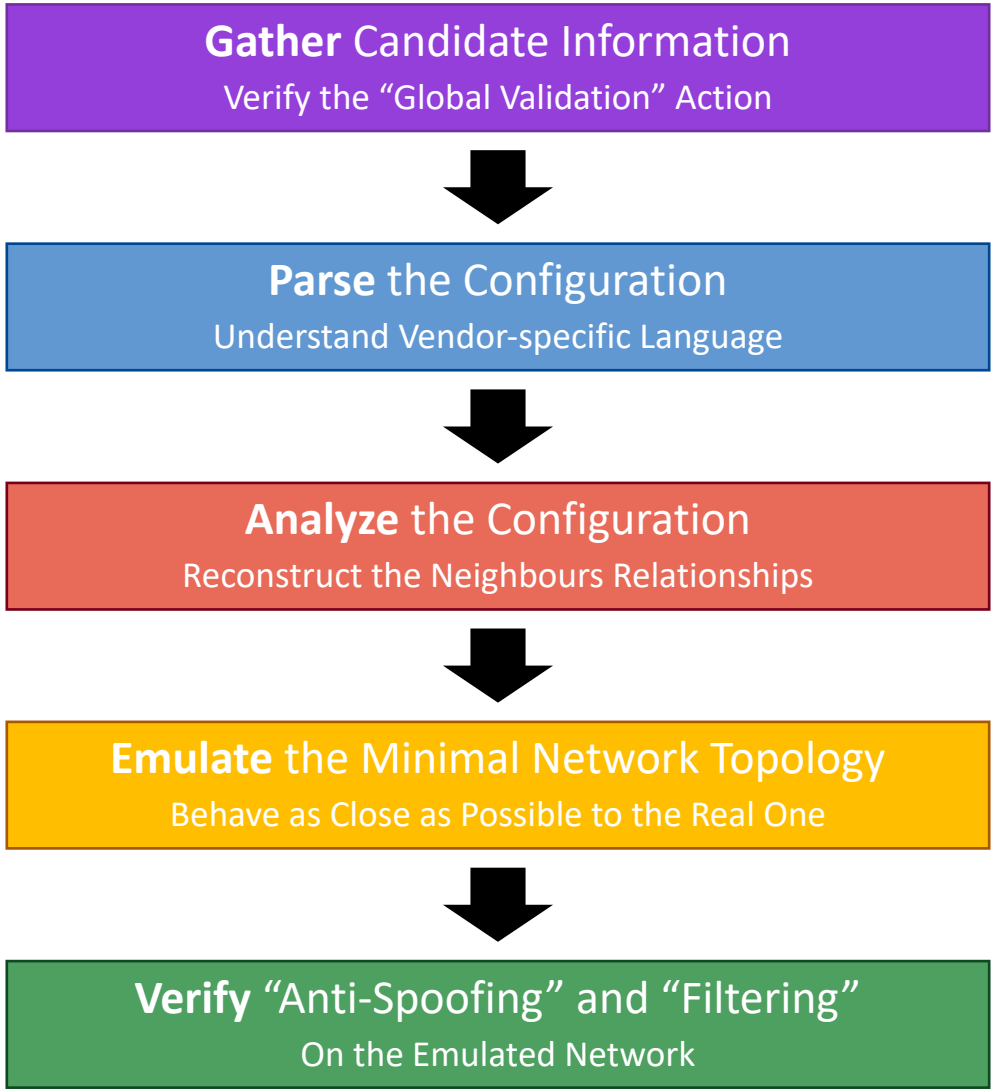
Require complex modelling

Emulation!

- ✓ **Run real software and configuration**
- ✓ **No need for creating complex models**
- ✓ **Operator friendly environment**

ROSE-T: How Does It Work?

Routing Security Tool
Rose-T

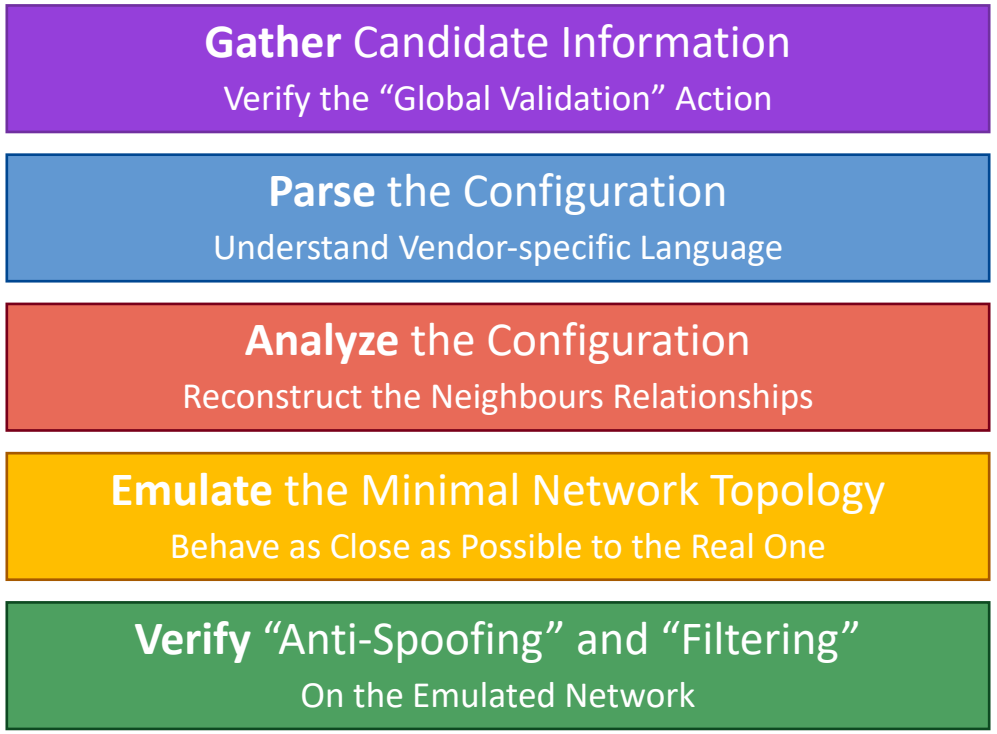


ROSE-T: ROuting SEcurity Tool

Routing Security Tool
Rose-T

Trust No One approach

Run ROSE-T locally to perform the self-assessment of the configuration



ROSE-T: ROuting SEcurity Tool

Routing Security Tool
Rose-T

Trust No One approach

Run ROSE-T locally to perform the self-assessment of the configuration

Gather Candidate Information
Verify the "Global Validation" Action

Parse the Configuration
Understand Vendor-specific Language

Analyze the Configuration
Reconstruct the Neighbours Relationships

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network

From the production's configurations

To a digital twin for verifying actions on an emulated network

ROSE-T: ROuting SEcurity Tool

Routing Security Tool

Rose-T

Trust No One approach

Run ROSE-T locally to perform the self-assessment of the configuration

What is ROSE-T able to do now?

Gather Candidate Information

Verify the "Global Validation" Action

Parse the Configuration

Understand Vendor-specific Language

Analyze the Configuration

Reconstruct the Neighbours Relationships

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One

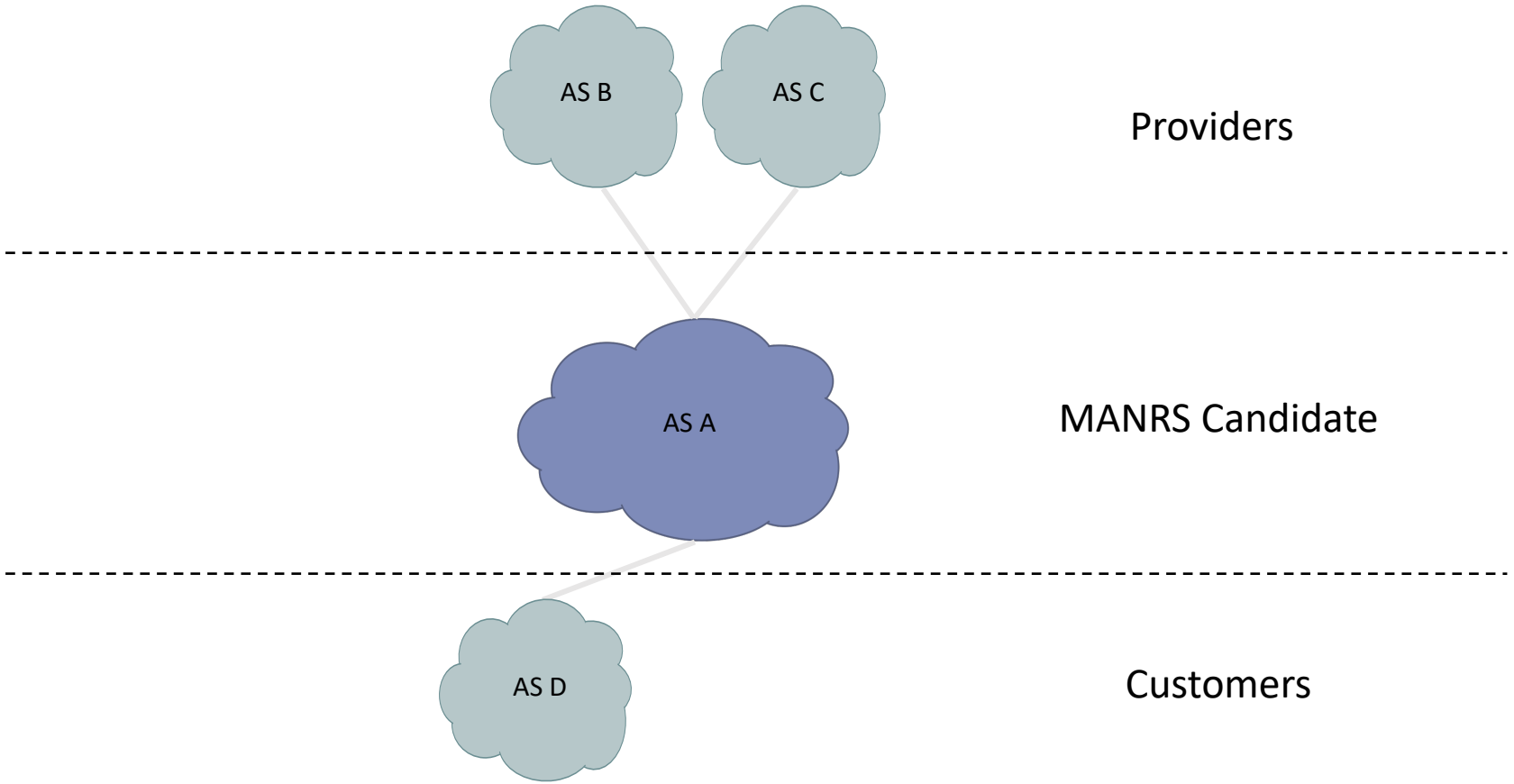
Verify "Anti-Spoofing" and "Filtering"

On the Emulated Network

From the production's configurations

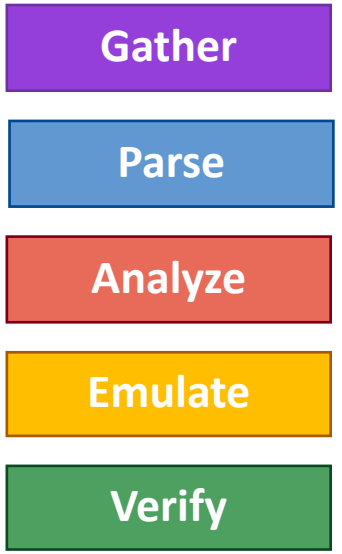
To a digital twin for verifying actions on an emulated network

ROSE-T: An Example Network



ROSE-T – Step-by-Step

Routing Security Tool
Rose-T



ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Gather Candidate Information
Verify the “Global Validation” Action

IRR Entry
RPSLng

RIB Dump

Routes originated by AS A

Parse
Analyze
Emulate
Verify

- Verify that the networks announced to transits are in the IRR Entry
- Verify that the networks in the IRR Entry are announced to transits

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Parse the Configuration
Understand Vendor-specific Language

Vendor-specific Configuration

Agnostic Format

Gather

Analyze

Emulate

Verify

Before: we exploited Batfish for **parsing vendor configurations**

- ✓ Good for vendors already supported
- ✗ Difficult to extend for new vendors
- ✗ Do not support IPv6

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Parse the Configuration
Understand Vendor-specific Language

Vendor-specific Configuration

Agnostic Format

Gather

Analyze

Emulate

Verify

Now: we developed a **custom parser** for vendor configurations

- We need to extract few information
- Facilitate the integration of new vendors

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Analyze the Configuration
Reconstruct the Neighbours Relationships

Agnostic Format

Gather

Parse

Emulate

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Analyze the Configuration
Reconstruct the Neighbours Relationships

Agnostic Format

What are their relationships?

IRR Entry
RPSLng

Gather

Parse

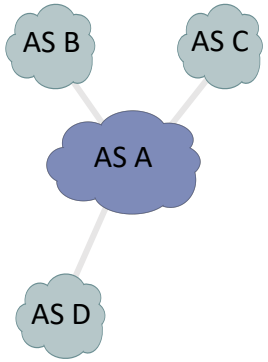
Emulate

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Analyze the Configuration
Reconstruct the Neighbours Relationships



Intermediate Representation

IRR Entry
RPSLng

Gather

Parse

Emulate

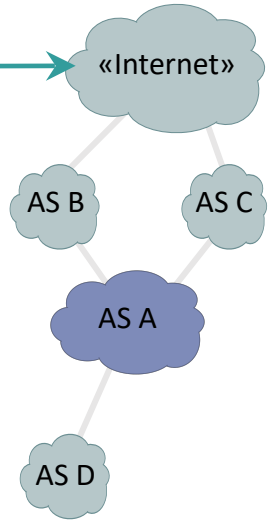
Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Analyze the Configuration
Reconstruct the Neighbours Relationships

Dummy OTT connected to all providers



Intermediate Representation

IRR Entry
RPSLng

Gather

Parse

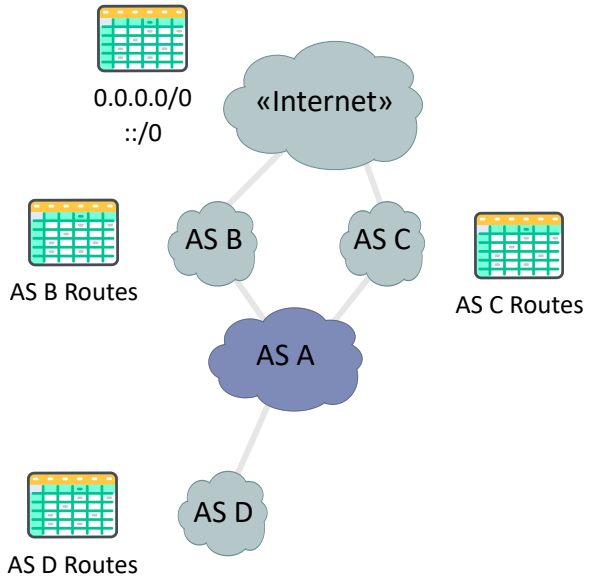
Emulate

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Analyze the Configuration
Reconstruct the Neighbours Relationships



Intermediate Representation

RIB Dump

Gather

Parse

Emulate

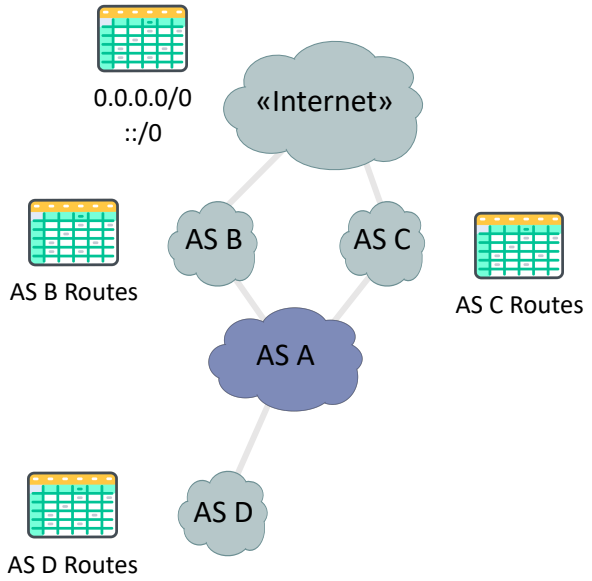
Verify

ROSE-T also supports multi-hop peerings!

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Intermediate Representation

Gather

Parse

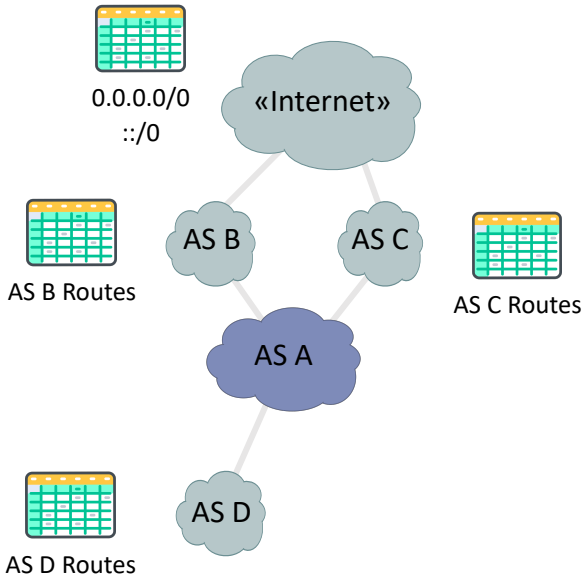
Analyze

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Intermediate Representation

Kathará

Gather

Parse

Analyze

Verify

Kathará - What is it?

Routing Security Tool
Rose-T

A container-based network emulator

Based on Docker containers

Can run on Kubernetes to scale up the emulation in a cluster

Open-source project

Almost 100K downloads

400+ stars on GitHub

Widely adopted for academic teaching and research

Used in 30 different courses, in more than 20 universities and 12 countries

Several publications and framework based on Kathará

ROSE-T – Why Kathará ?

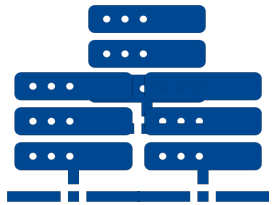
Routing Security Tool
Rose-T

Lightweight

- ✓ Minimal resource usage
- ✓ Fast startup

Python APIs

- ✓ Easy programming interface
- ✓ Easy to extend



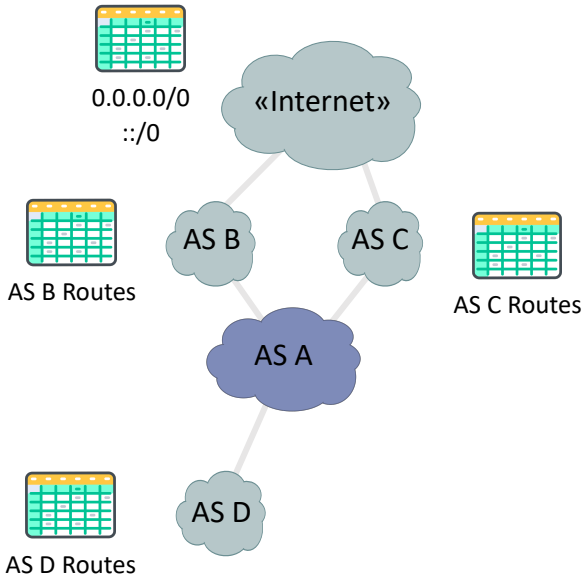
Scalable

- ✓ Docker on single host
- ✓ K8s on a cluster

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Intermediate Representation

Kathará

Gather

Parse

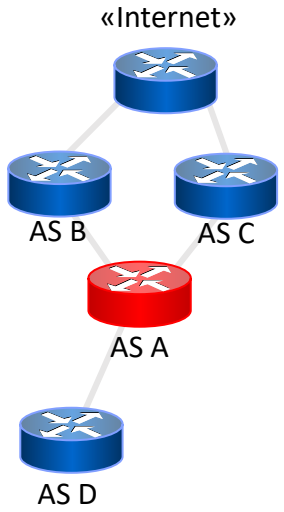
Analyze

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Runnable Network Scenario

Kathará

Gather

Parse

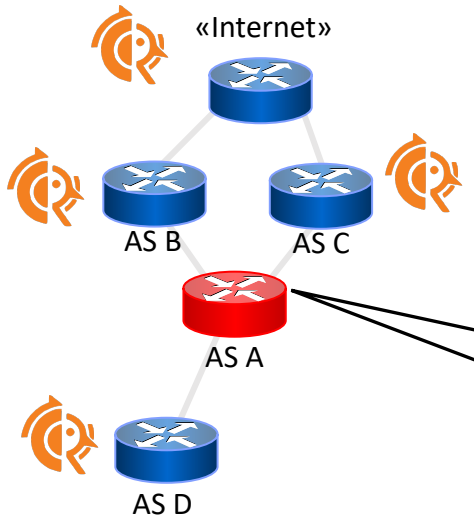
Analyze

Verify

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Emulate the Minimal Network Topology
Behave as Close as Possible to the Real One



Runnable Network Scenario

Kathará

Gather

Parse

Analyze

Verify

CISCO JUNIPER NETWORKS MikroTik

More to come…

Vendor Container

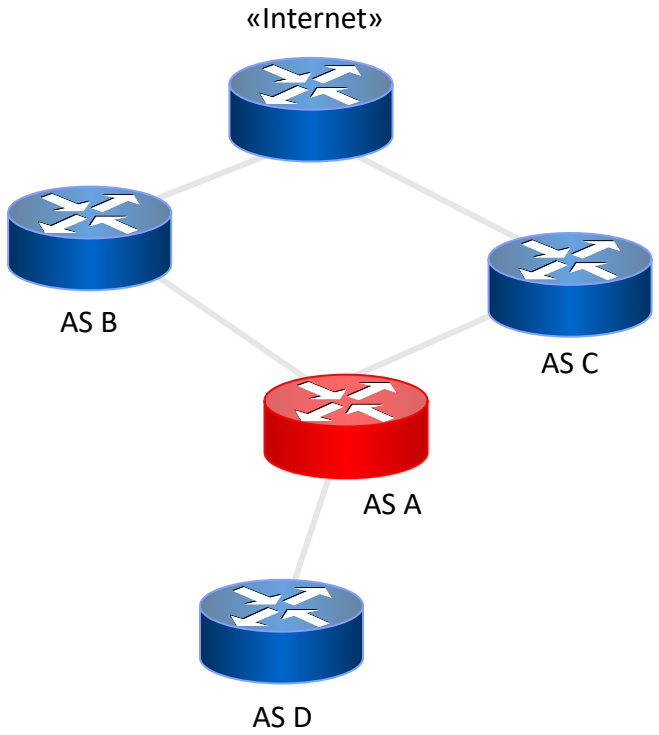
From the last update we added the support to RouterOS

ROSE-T can easily be extended to support other vendors

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Gather

Parse

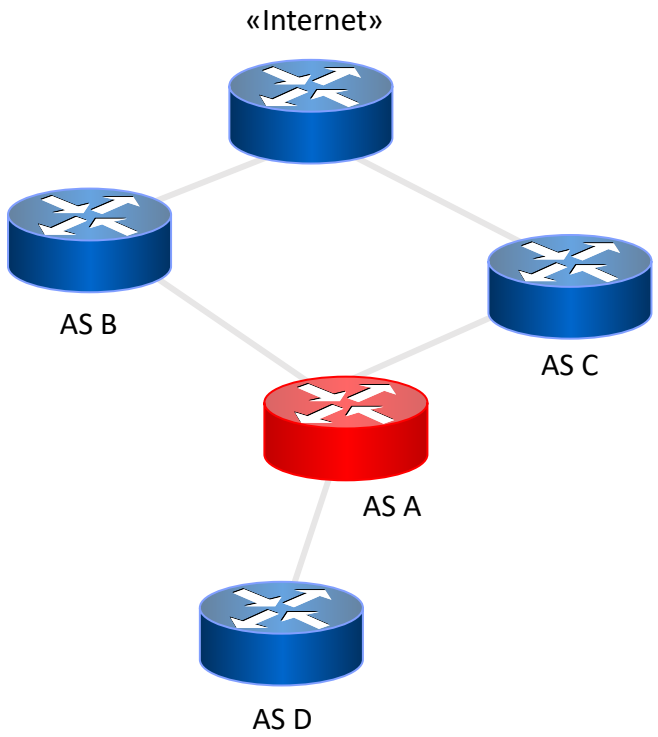
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

Gather

Parse

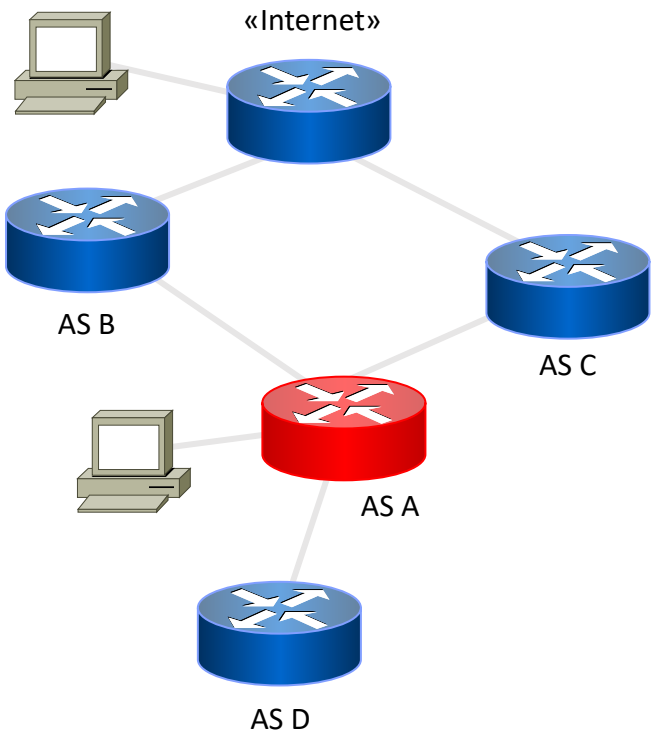
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

Gather

Parse

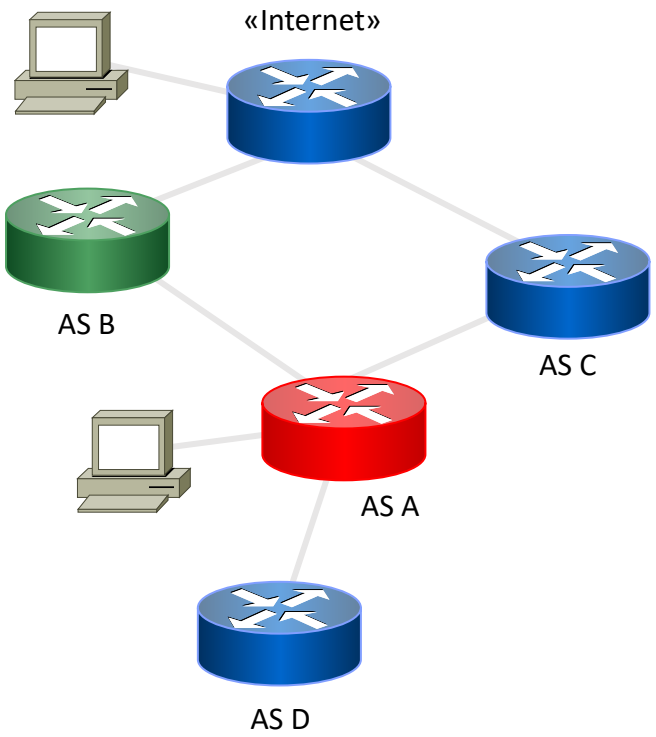
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

For each Provider:

Gather

Parse

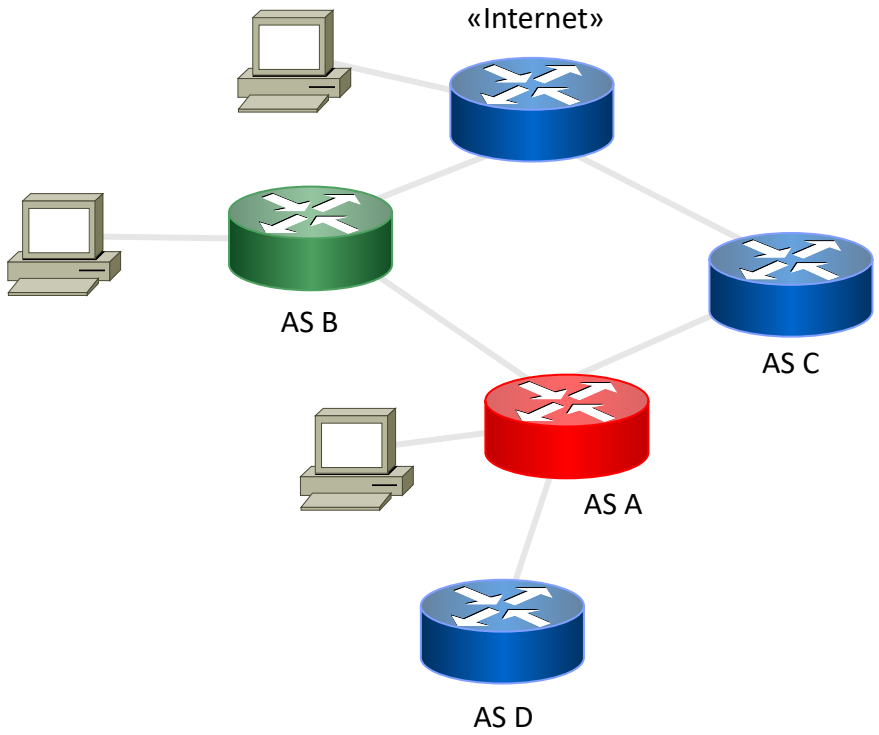
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client

Gather

Parse

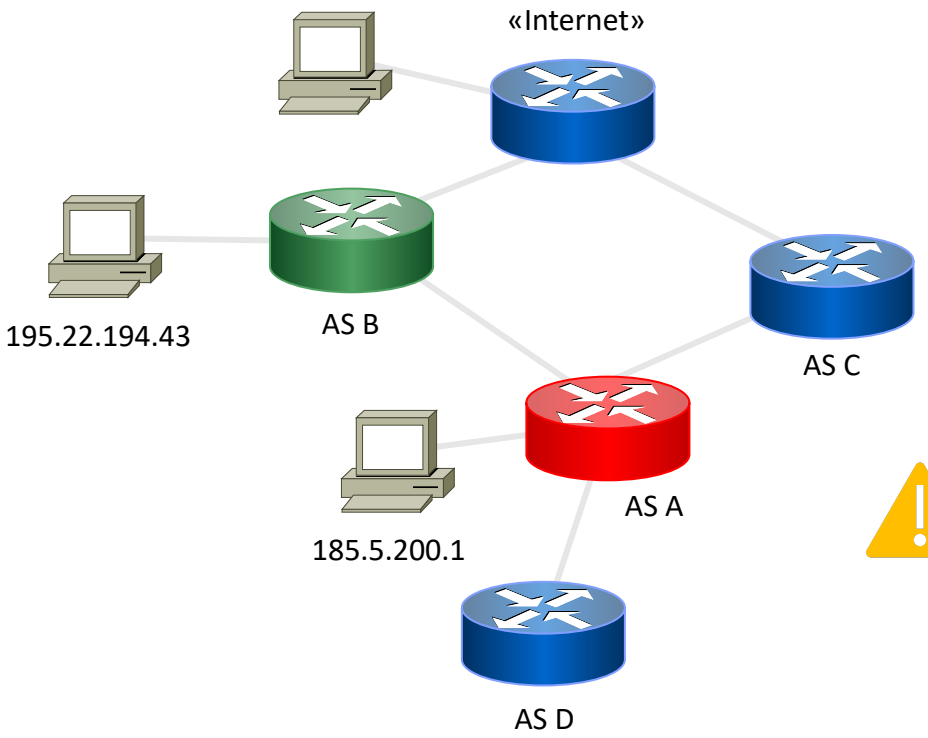
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client

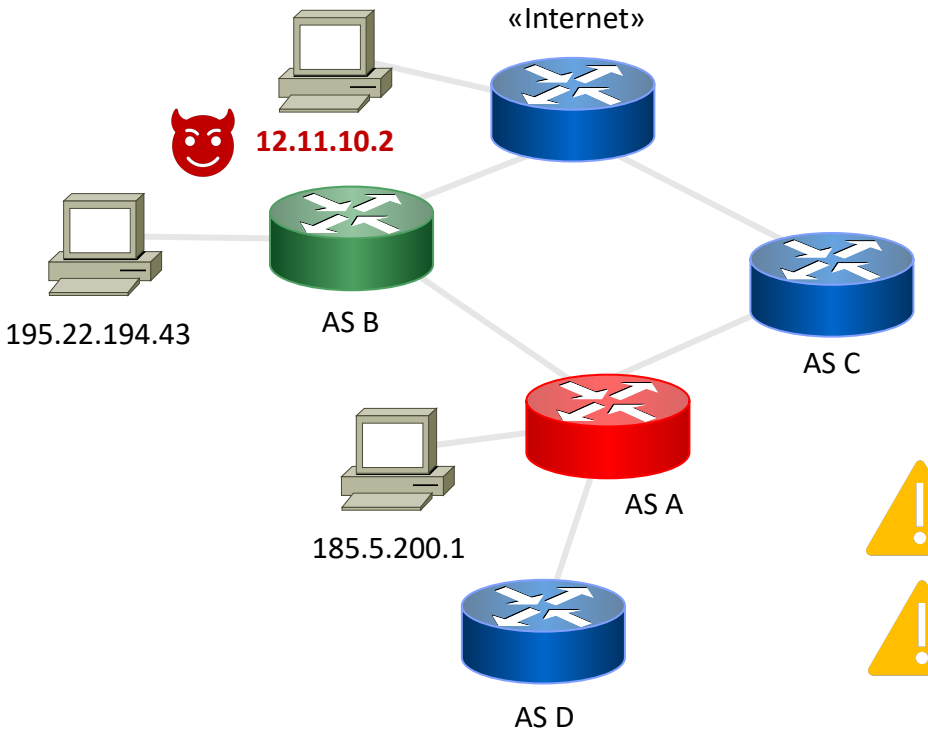
Gather
Parse
Analyze
Emulate

Carefully choose subnets that are correctly announced and reachable

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client

Gather
Parse
Analyze
Emulate

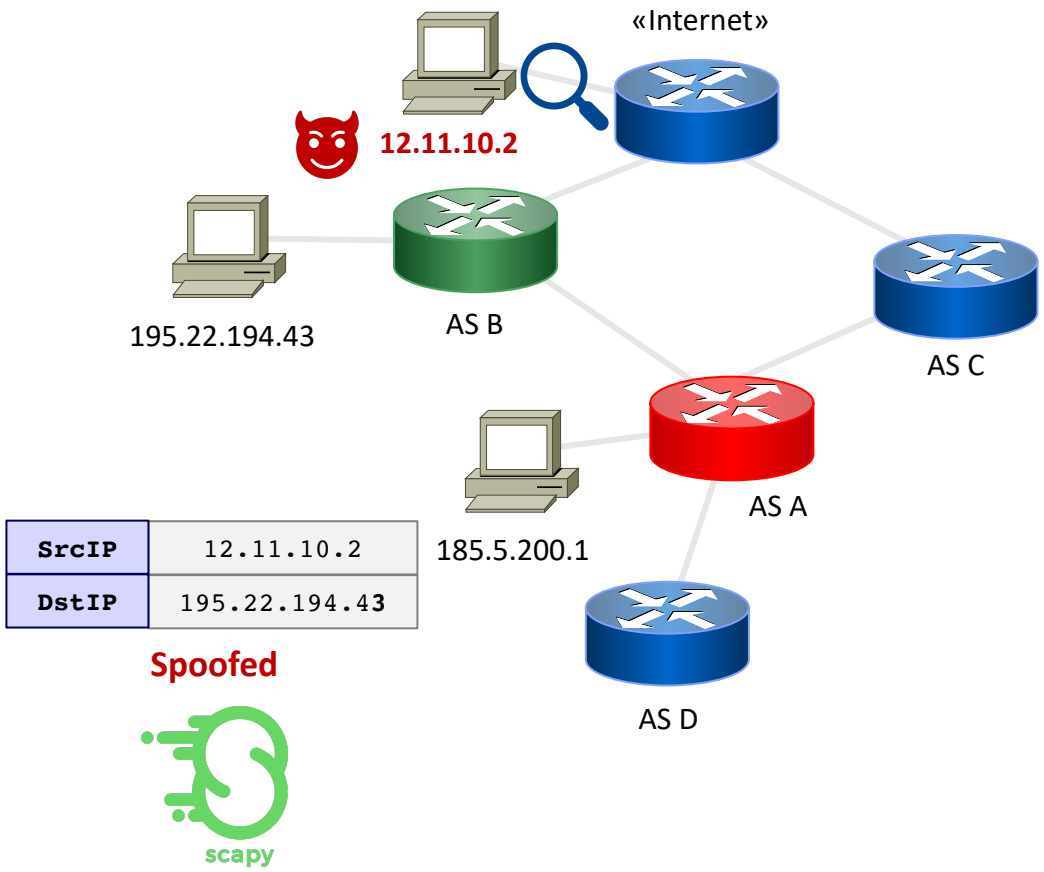
Carefully choose subnets that are correctly announced and reachable

Select a non-overlapping network for the "Internet" client

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

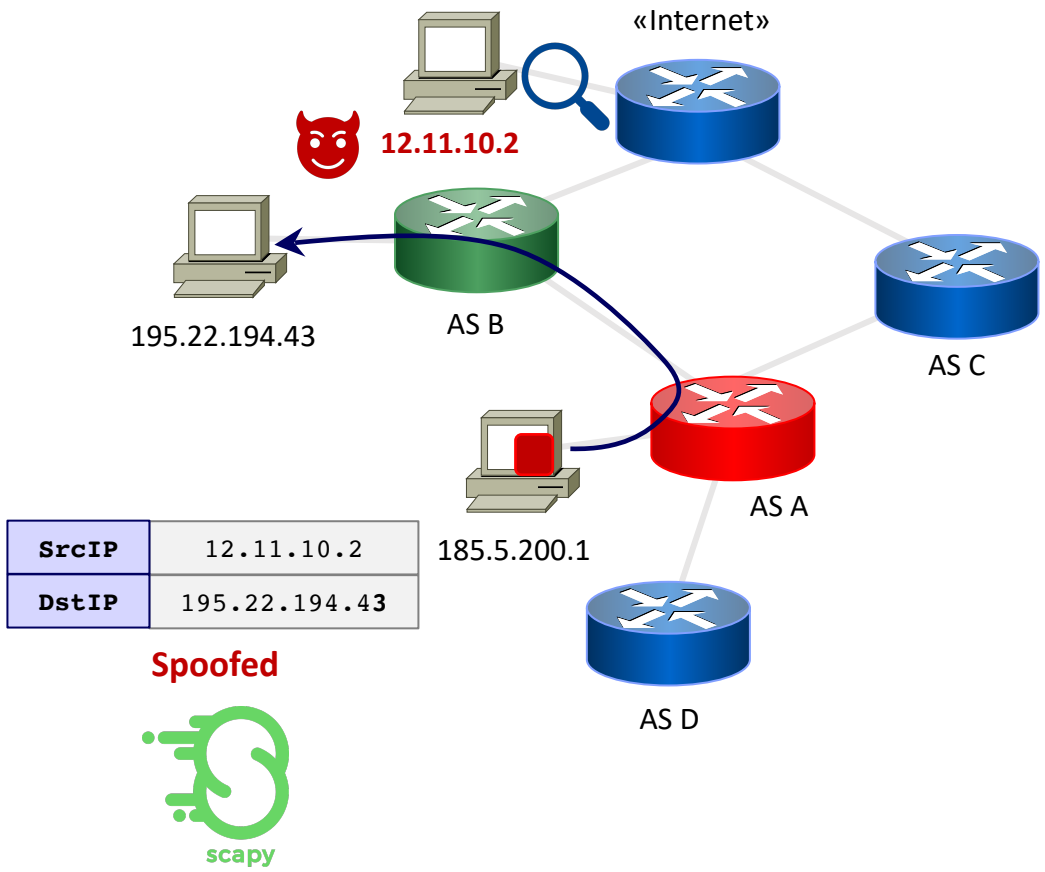
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

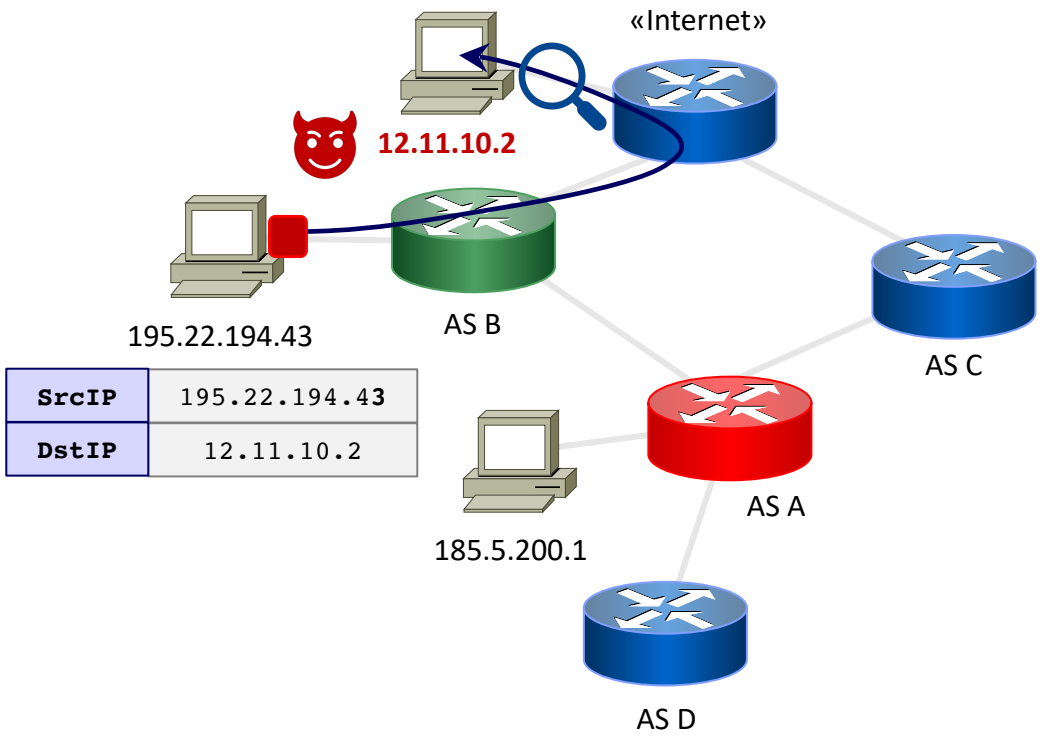
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

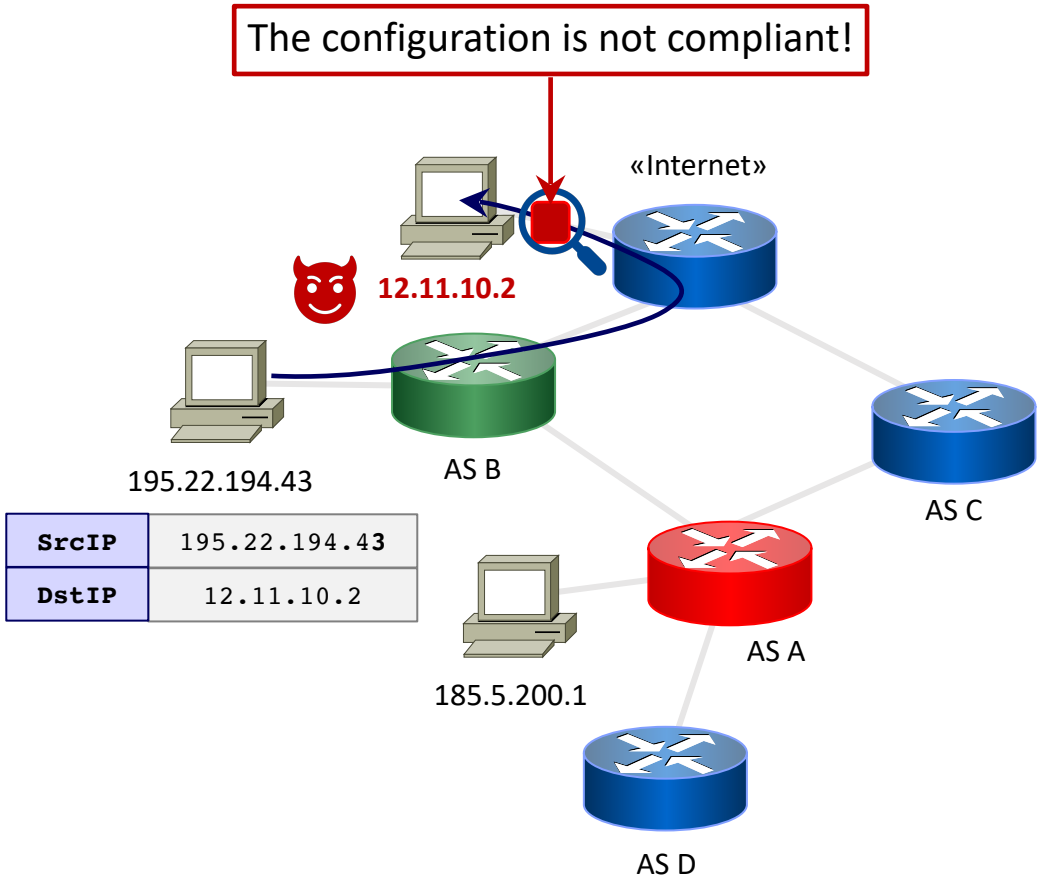
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

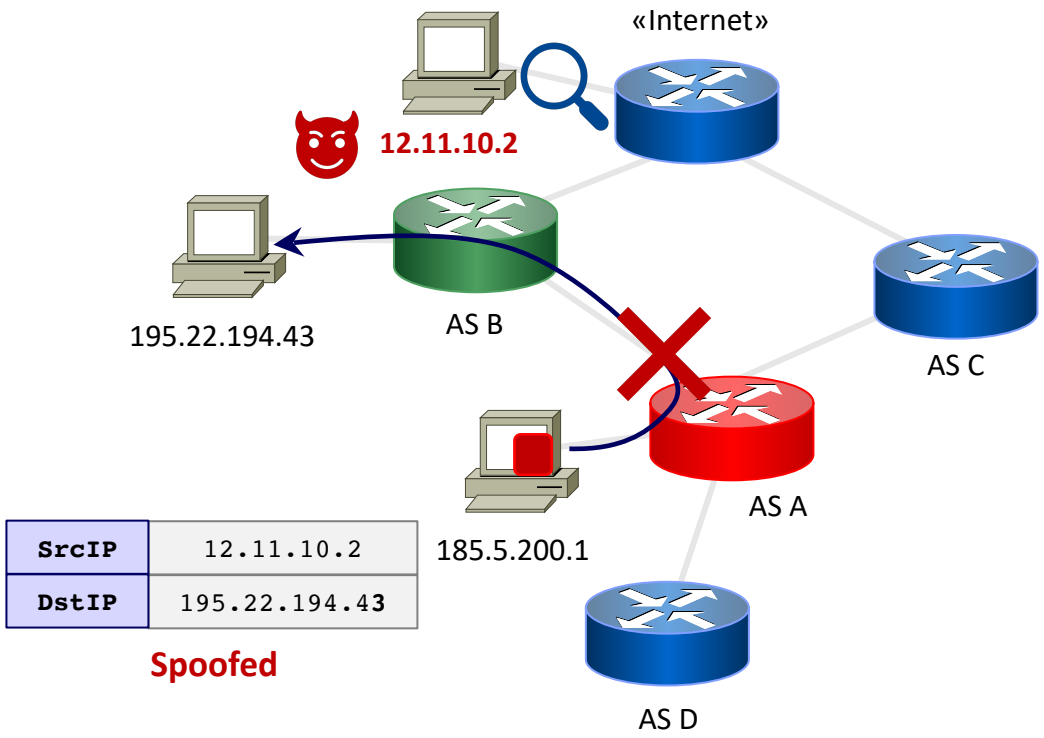
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

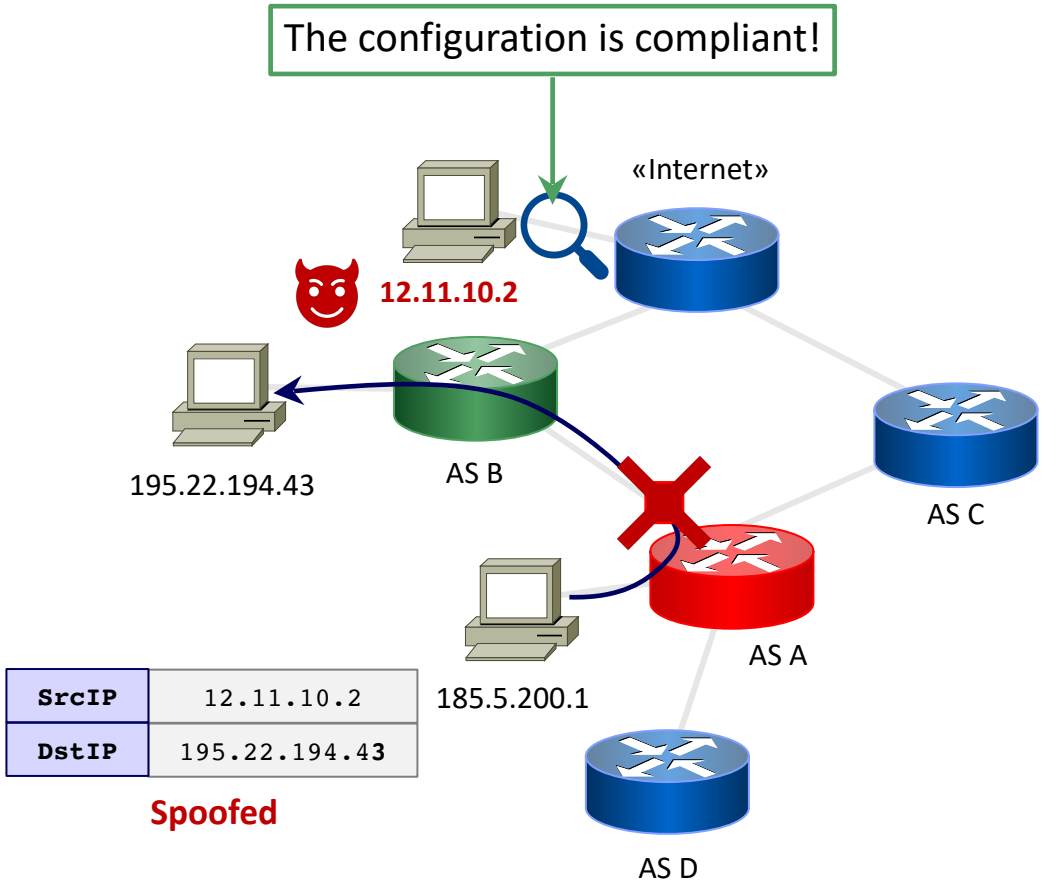
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

Gather

Parse

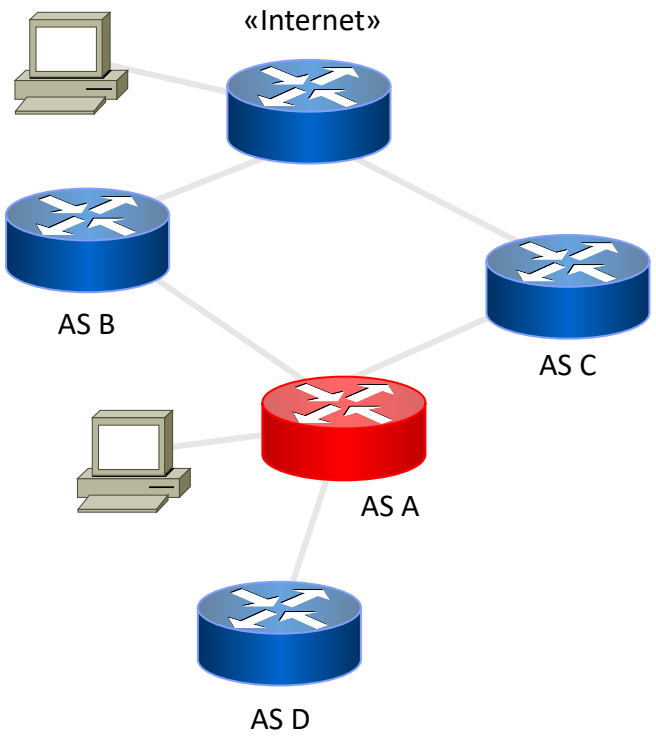
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

Gather

Parse

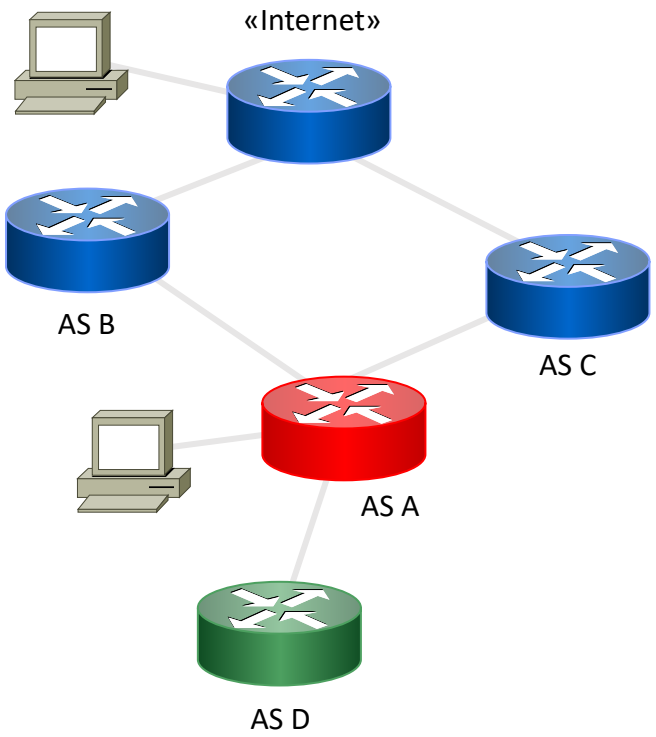
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

For each Customer:

Gather

Parse

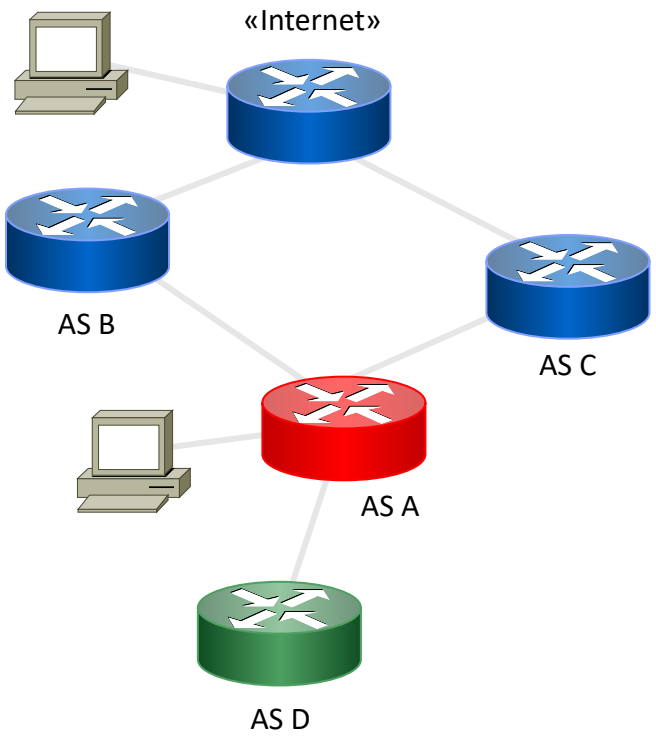
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate

Gather

Parse

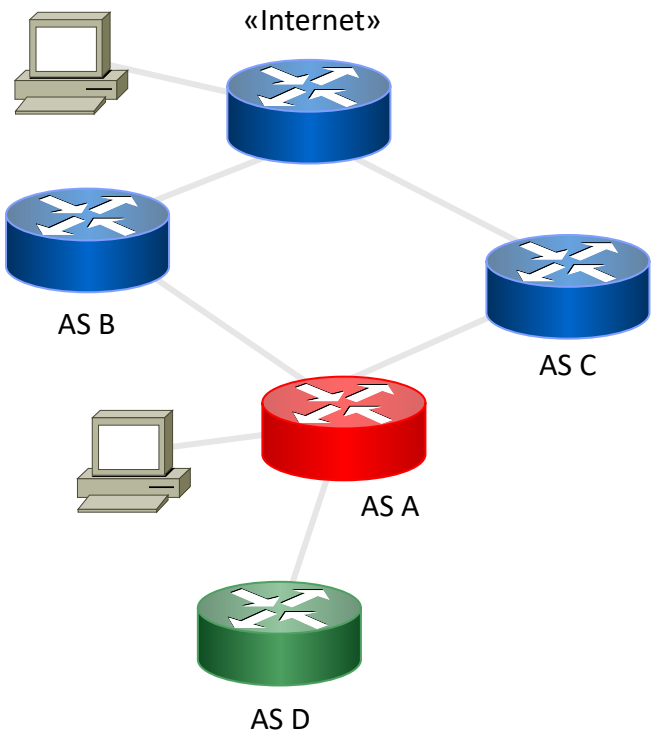
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate

12.11.10.0/24

Gather

Parse

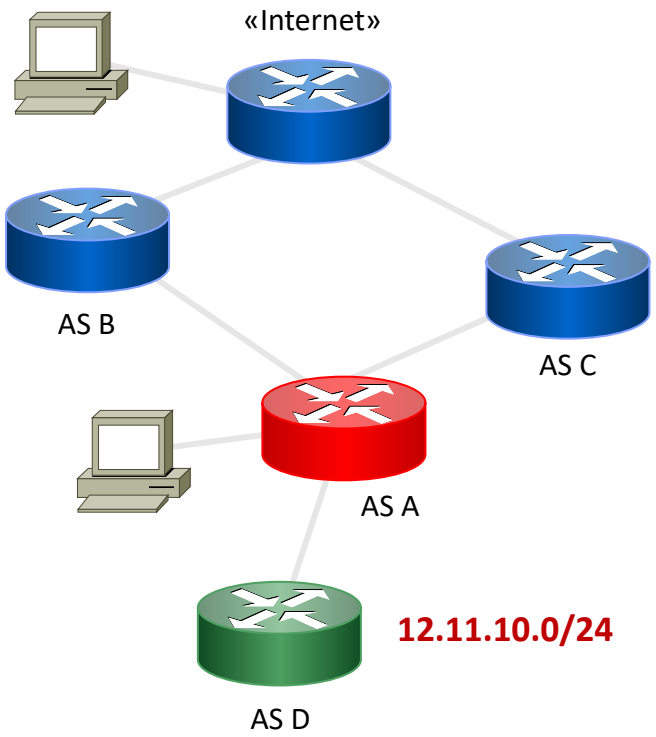
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate

Gather

Parse

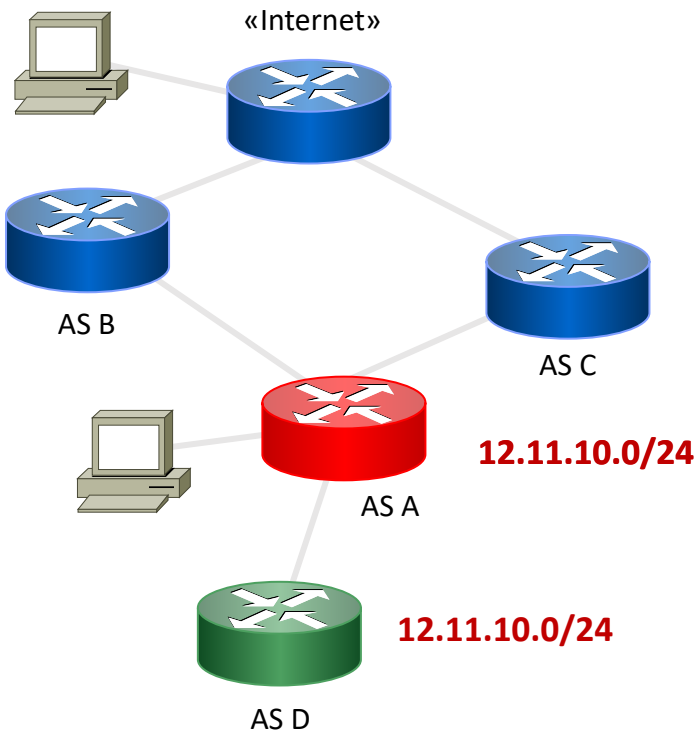
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait

Gather

Parse

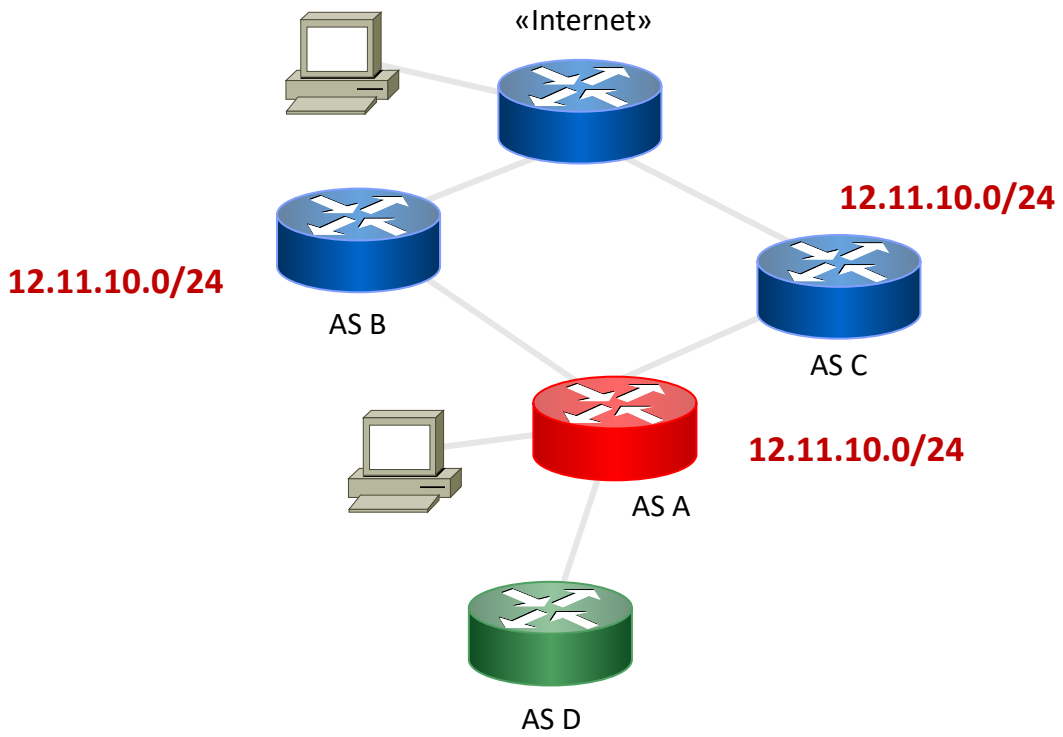
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait

Gather

Parse

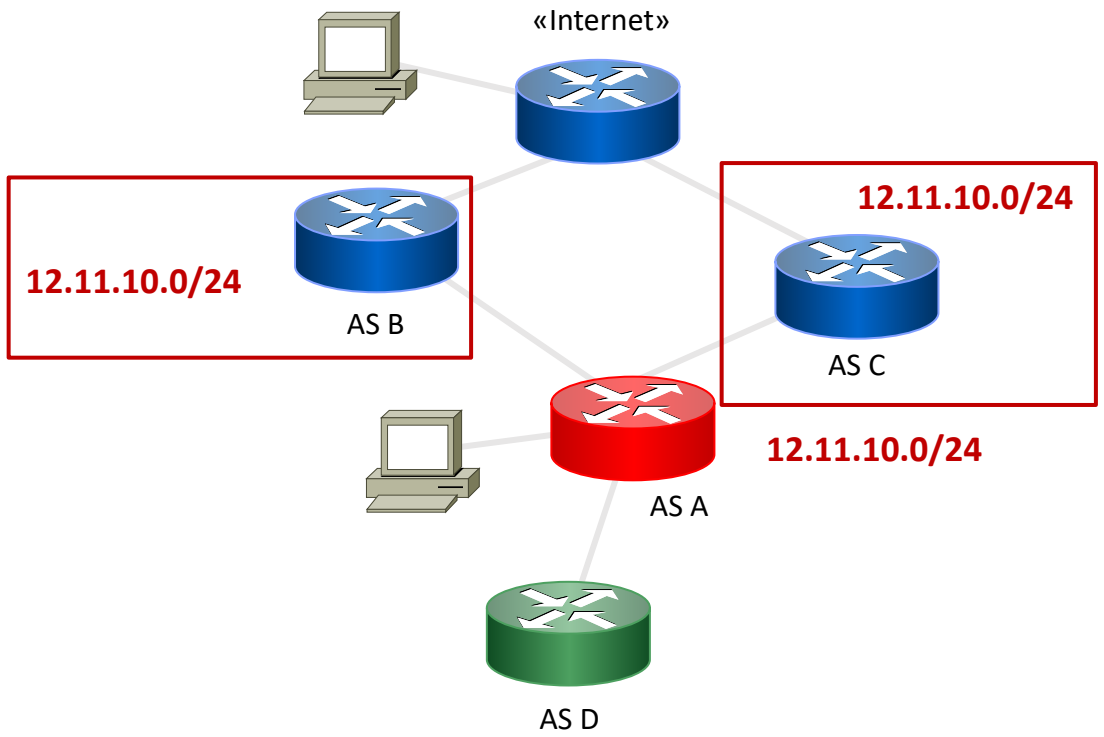
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
ROSE-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait
3. Check the provider's received routes
   - Using the FRRouting control plane

Gather

Parse

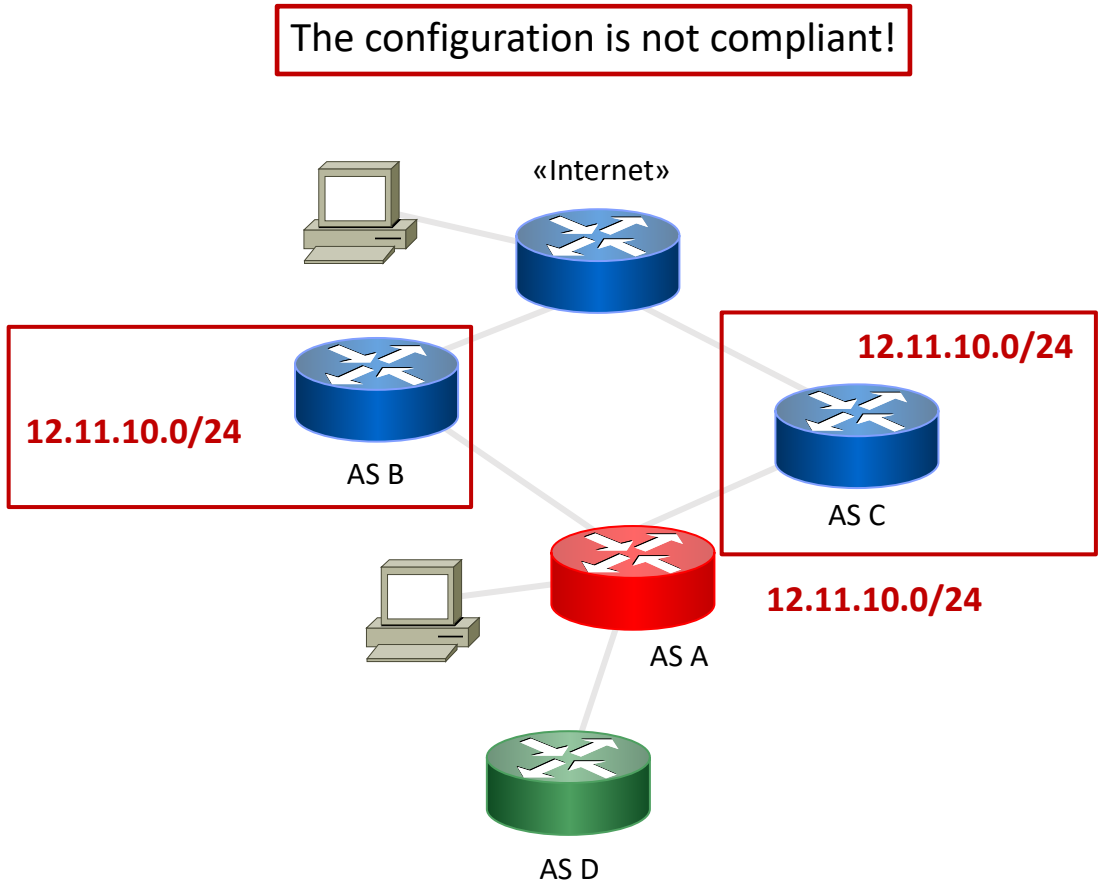
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait
3. Check the provider's received routes
   - Using the FRRouting control plane

Gather

Parse

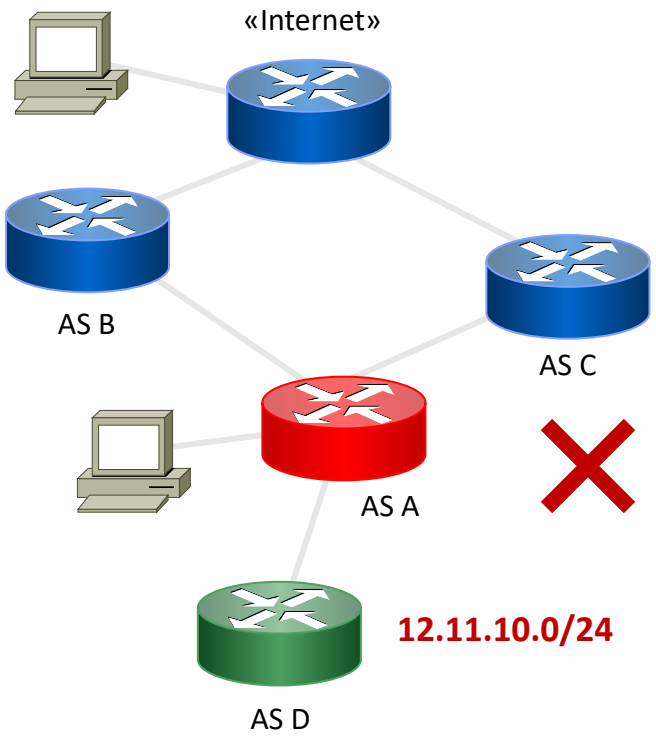
Analyze

Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify "Anti-Spoofing" and "Filtering"
On the Emulated Network



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait
3. Check the provider's received routes
   - Using the FRRouting control plane

Gather

Parse

Analyze

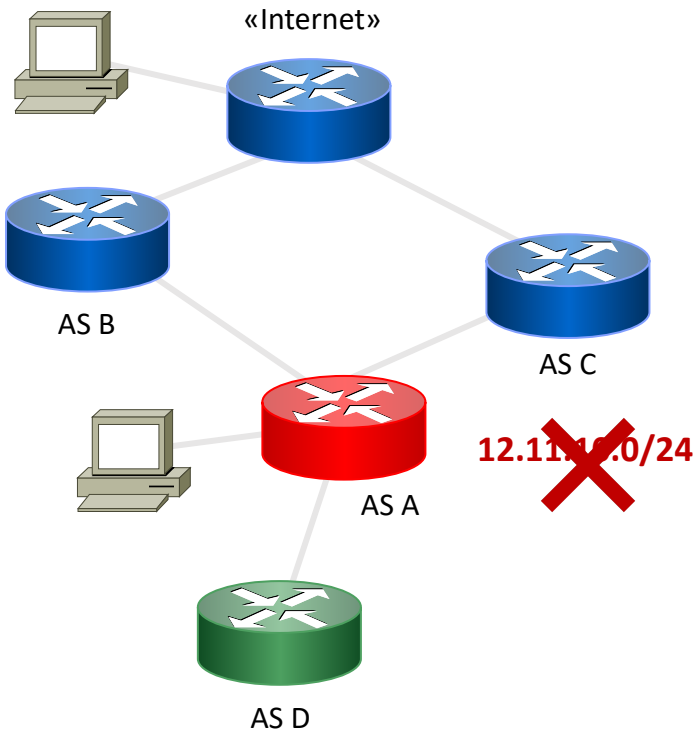
Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

Verify “Anti-Spoofing” and “Filtering”
On the Emulated Network

The configuration is compliant!



Filtering

For each Customer:

1. Select non-overlapping subnet
   - Announced to the Candidate
2. Announce the subnet & wait
3. Check the provider’s received routes
   - Using the FRRouting control plane

Gather

Parse

Analyze

Emulate

ROSE-T – Updates

Routing Security Tool

Rose-T

From the last update:

We developed a **custom parser** for configurations to easily integrate new vendors

We added the support for **MikroTik RouterOS**

We unified all the checks in the Python code

Before the **Global Information** action was implemented separately

ROSE-T – Current Limitations

Routing Security Tool
Rose-T

Support only single-router configurations

- We are starting to work on multi-routers!
- This is the next step!

Consider only actions for network operators

- It can be extended to IXPs, CDNs and Cloud Providers

Extend ROSE-T for MANRS+

- We already presented a proposal to the MANRS+ WG

Extend the support to other vendors

Contacts

Routing Security Tool
Rose-T

Mariano Scazzariello

RISE Research Institutes of Sweden

Antonio Prado

“G. D’Annunzio” University

Tommaso Caiazzi

Roma Tre University

Read more about ROSE-T on our blog post on MANRS

https://manrs.org/2024/03/verify-manrs-compliance-automatically-with-ROSE-T/

Contribute!