Routing Security Tool

Rose-T

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

[*] KTH Royal Institute of Technology, Sweden

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

Why is Routing Security Crucial Nowadays?

Cyber Threats

Business Continuity

Sensitive Data

Why is Routing Security Crucial Nowadays?

Cyber Threats

Business Continuity

Sensitive Data

Routing Resilience Manifesto
(2014)

Why is Routing Security Crucial Nowadays?

Cyber Threats

Business Continuity

Sensitive Data

MANRS

MANRS

Mutually Agreed Norms for Routing Security

Guidelines and **best practices** to mitigate most common routing threats

MANRS proposes specific actions in **4 programs**:

1. **Network Operators**
2. **Internet Exchange Points**
3. **CDNs and Cloud Providers**
4. **Equipment Vendors**

MANRS Actions For Network Operators

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

Coordination

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

Global Validation

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

How Can a Network Operator Ensure the MANRS Compliance?

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?

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!

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!

How can we do that?

Simulation?

Good for testing how the network behaves in theory

Cannot consider real configurations and software

Require complex modelling

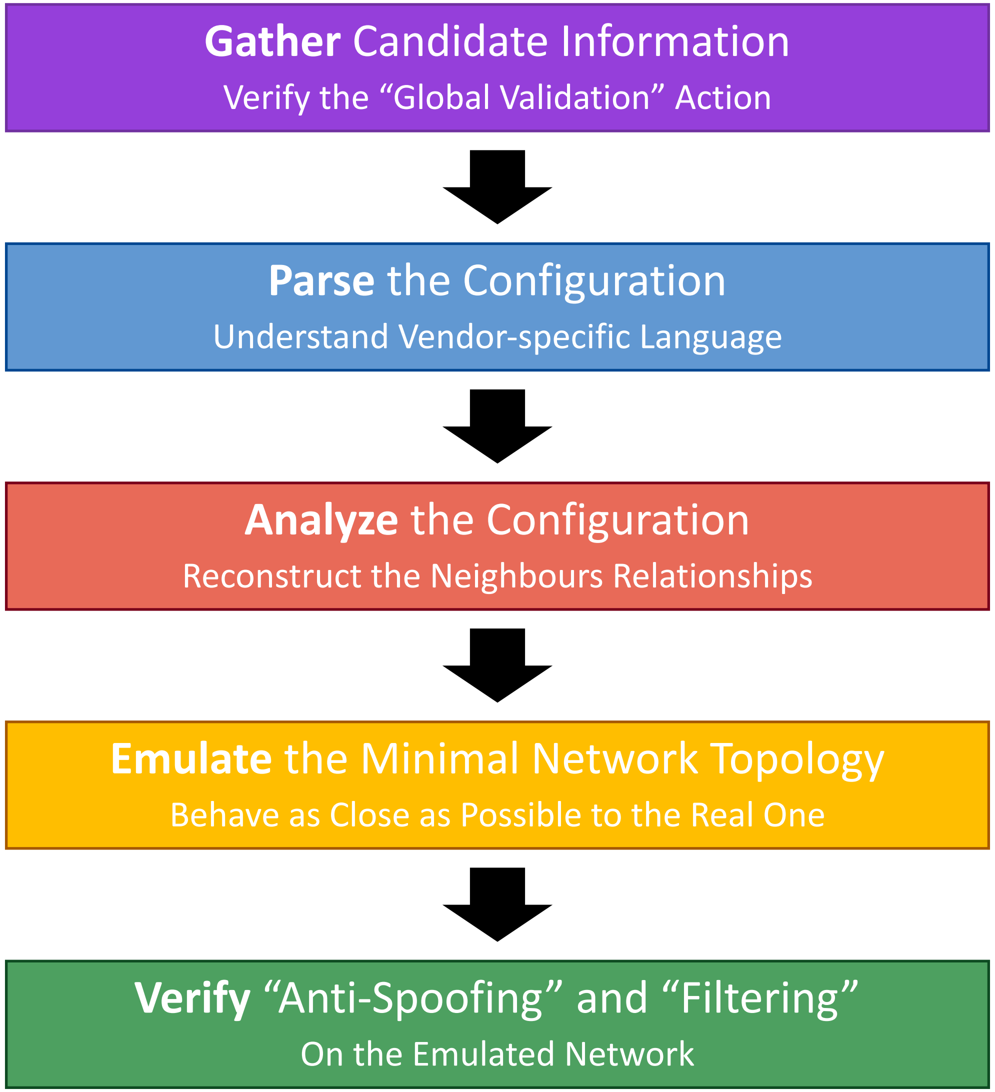
Emulation!

✓ Run real software and configuration

✓ No need for creating complex models

✓ Operator friendly environment

ROSE-T: How Does It Work?



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

ROSE-T: ROuting SEcurity Tool

The first **open-source** tool to automatically verify MANRS compliance

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

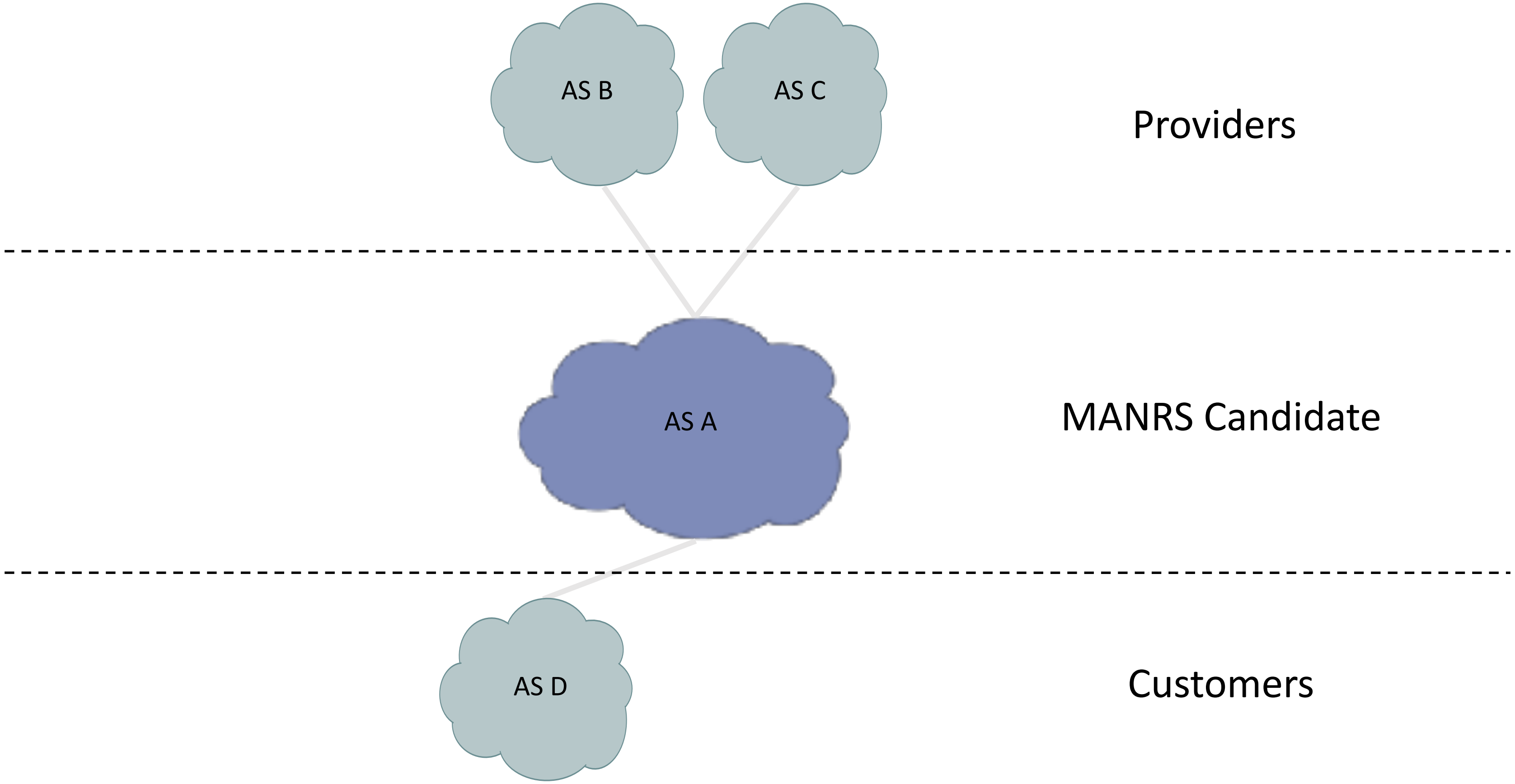
Analyze the Configuration
Reconstruct the Neighbours Relationships

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

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

ROSE-T: An Example Network

Routing Security Tool



ROSE-T – Step-by-Step

Gather

Parse

Analyze

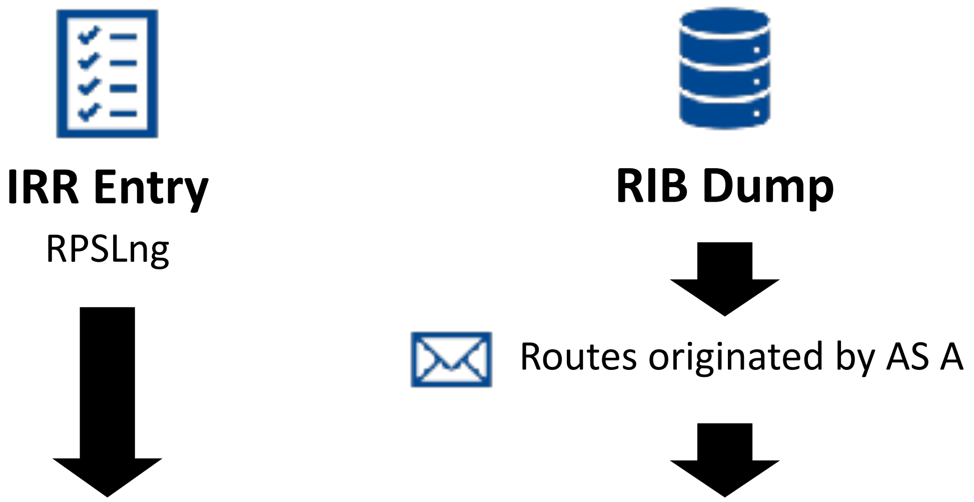
Emulate

Verify

ROSE-T – Step-by-Step

Gather Candidate Information

Verify the “Global Validation” Action



IRR Entry

RPSLng

RIB Dump

Routes originated by AS A

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

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

Parse

Analyze

Emulate

Verify

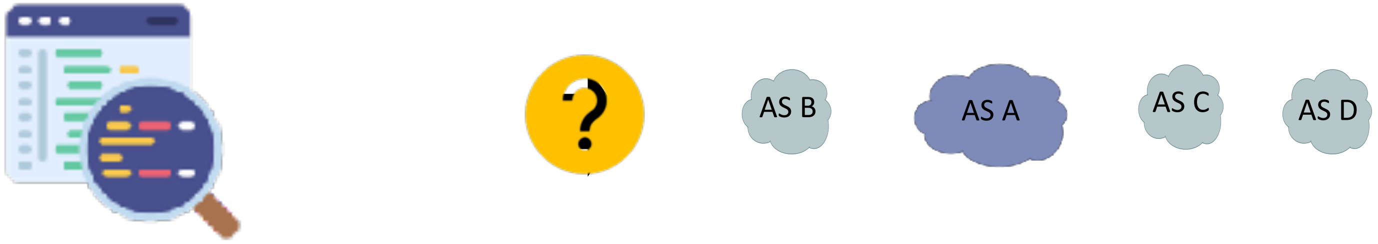
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Parse the Configuration

Understand Vendor-specific Language



Vendor-specific Configuration

Agnostic Format

Gather

Analyze

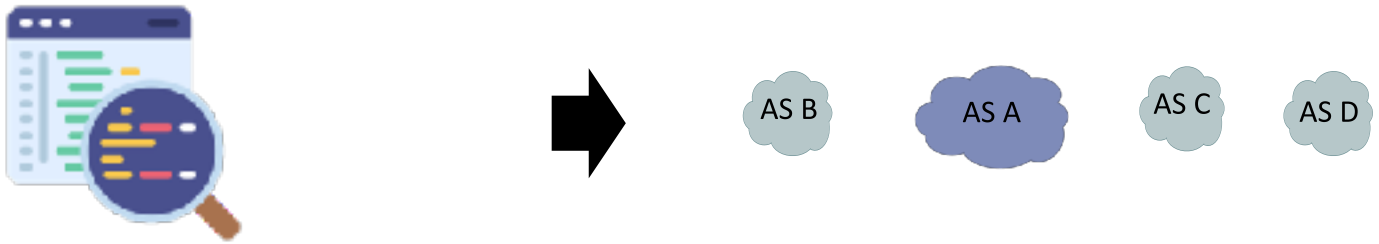
Emulate

Verify

Exploit what Batfish does best: **parsing vendor configurations**

ROSE-T – Step-by-Step

Parse the Configuration
Understand Vendor-specific Language



Vendor-specific Configuration

Agnostic Format

Exploit what Batfish does best: **parsing vendor configurations**

Take Batfish's output as a foundation

Enrich it with missing information

Gather

Analyze

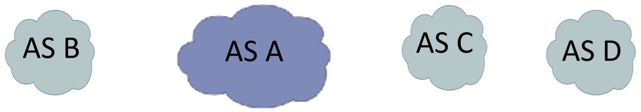
Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships



Agnostic Format

Gather

Parse

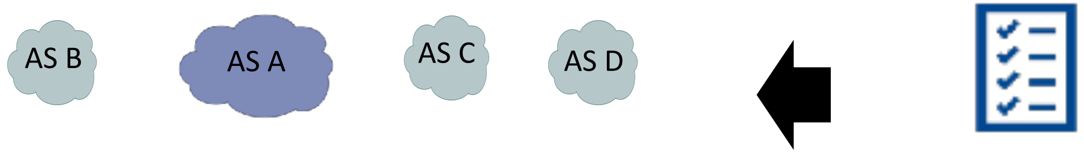
Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships



Agnostic Format

IRR Entry

RPSLng

? What are their relationships?

Gather

Parse

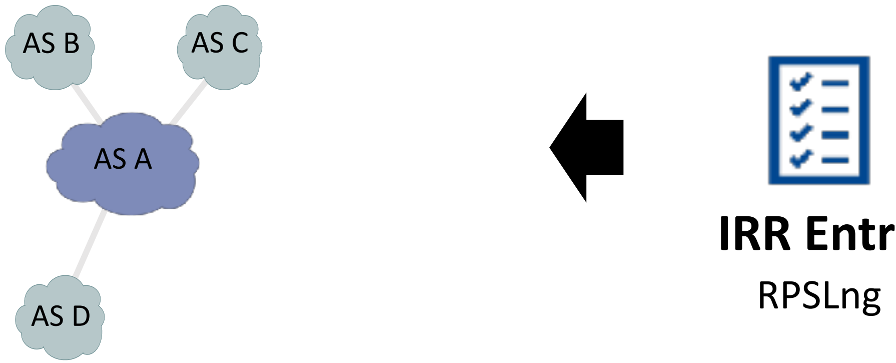
Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships



IRR Entry

RPSLng

Intermediate Representation

Gather

Parse

Emulate

Verify

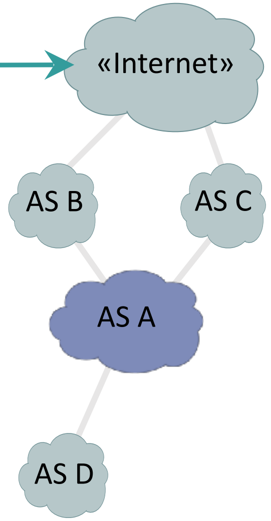
ROSE-T – Step-by-Step

Routing Security Tool

Analyze the Configuration

Reconstruct the Neighbours Relationships

Dummy OTT connected to all providers



Intermediate Representation

IRR Entry

RPSLng

Gather

Parse

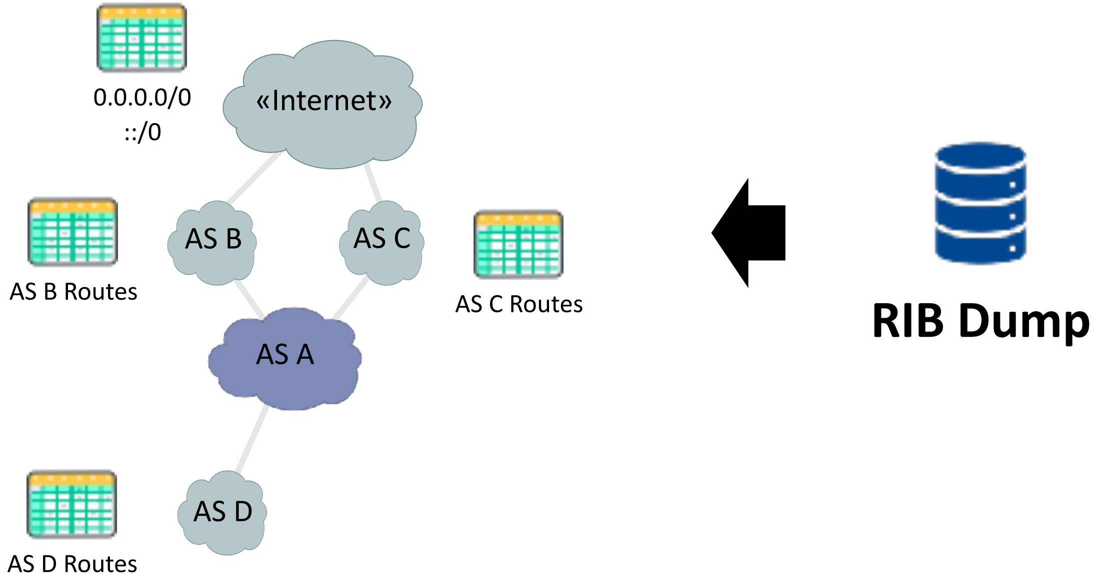
Emulate

Verify

ROSE-T – Step-by-Step

Analyze the Configuration

Reconstruct the Neighbours Relationships



Intermediate Representation

Gather

Parse

Emulate

Verify

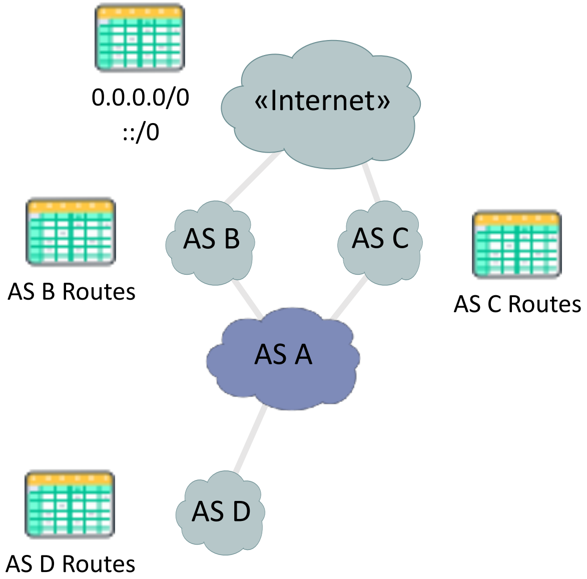
✓ ROSE-T also supports multi-hop peerings!

ROSE-T – Step-by-Step

Routing Security Tool

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Intermediate Representation

Gather

Parse

Analyze

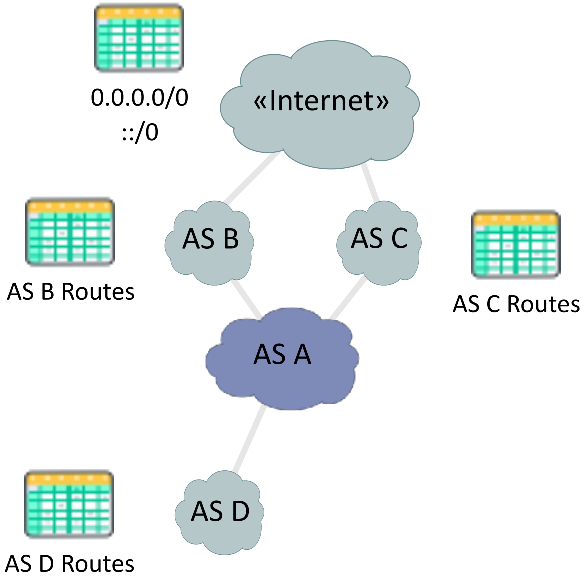
Verify

ROSE-T – Step-by-Step

Routing Security Tool

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Intermediate Representation

Gather

Parse

Analyze

Verify

Kathará - What is?

A container-based network emulator

Based on Docker containers

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

Open-source project developed at Roma Tre University

Almost 100K downloads

385 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

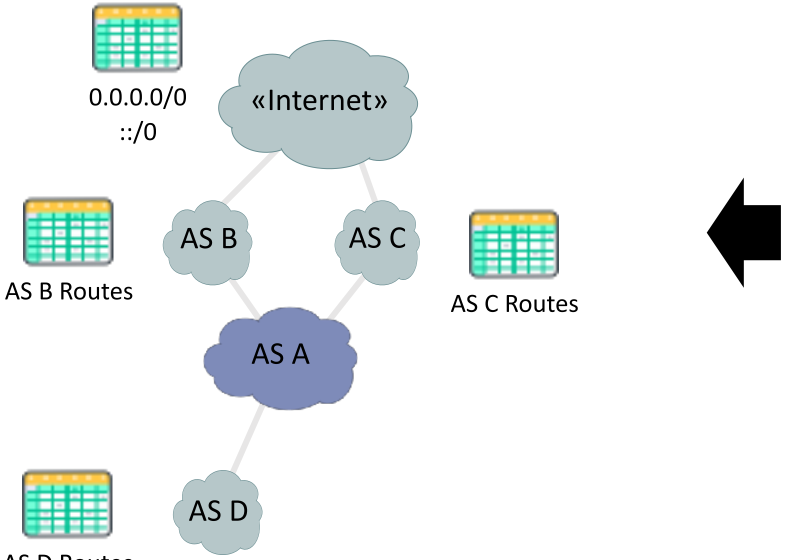
✓ K8s on a cluster

ROSE-T – Step-by-Step

Routing Security Tool

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Intermediate Representation

Kathará

Gather

Parse

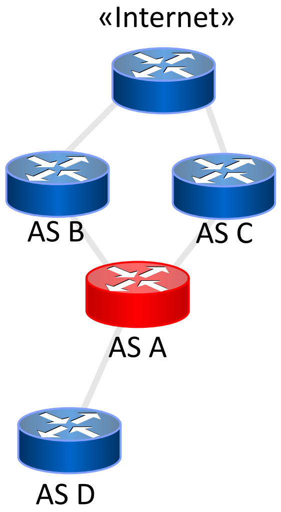
Analyze

Verify

ROSE-T – Step-by-Step

Emulate the Minimal Network Topology

Behave as Close as Possible to the Real One



Runnable Network Scenario

←

Kathará

Gather

Parse

Analyze

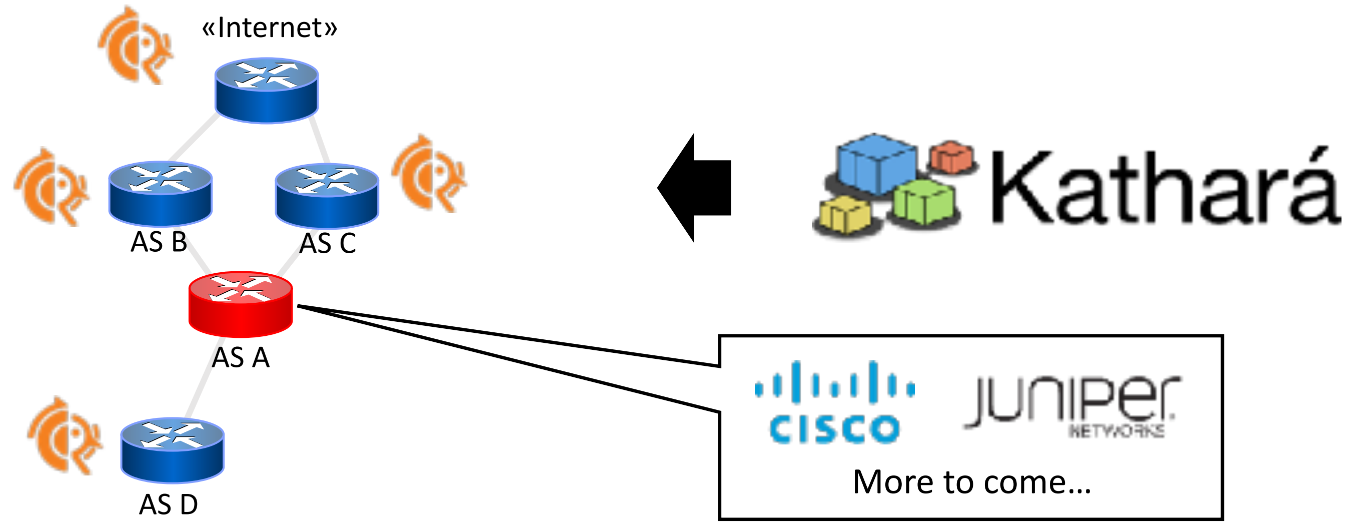
Verify

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

Vendor Container

Gather

Parse

Analyze

Verify

✓ ROSE-T can easily be extended to support other vendors

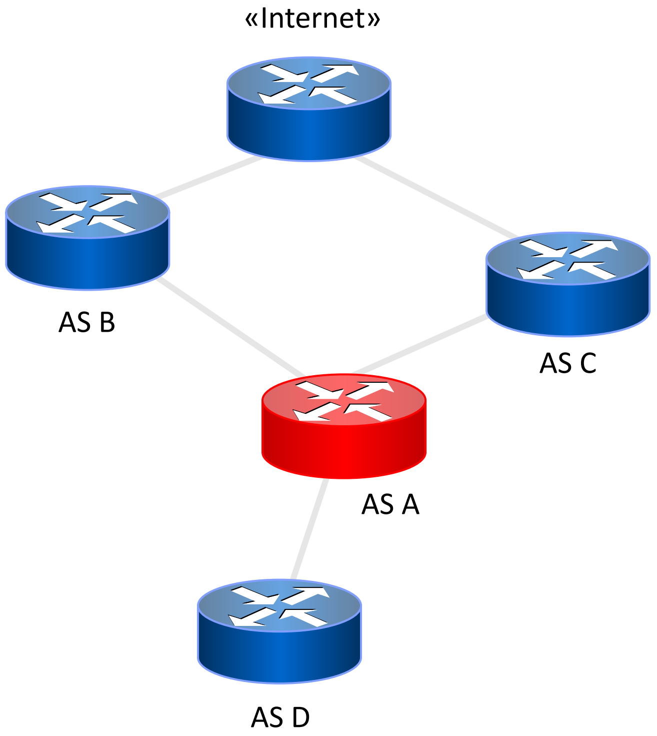
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Verify "Anti-Spoofing" and "Filtering"

On the Emulated Network



Gather

Parse

Analyze

Emulate

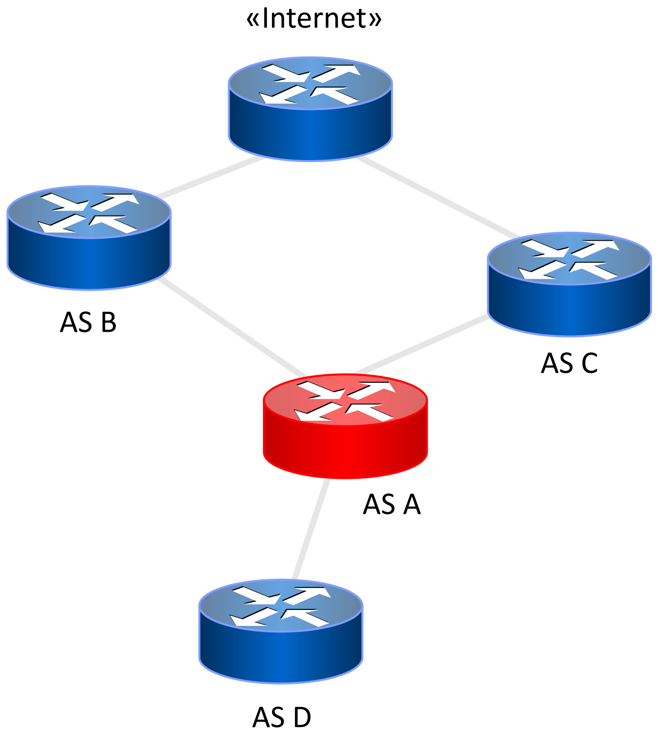
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Verify "Anti-Spoofing" and "Filtering"

On the Emulated Network



Anti-Spoofing

Gather

Parse

Analyze

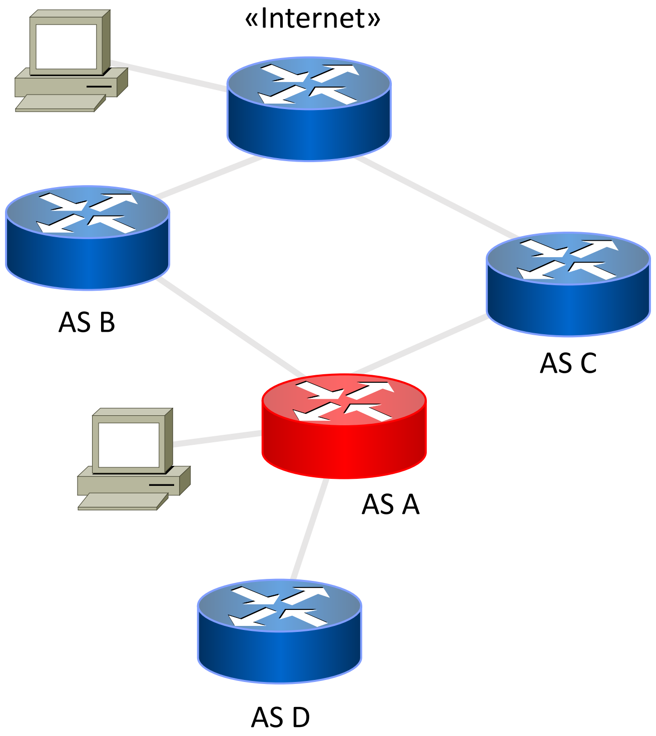
Emulate

ROSE-T – Step-by-Step

Routing Security Tool

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network



Anti-Spoofing

Gather

Parse

Analyze

Emulate

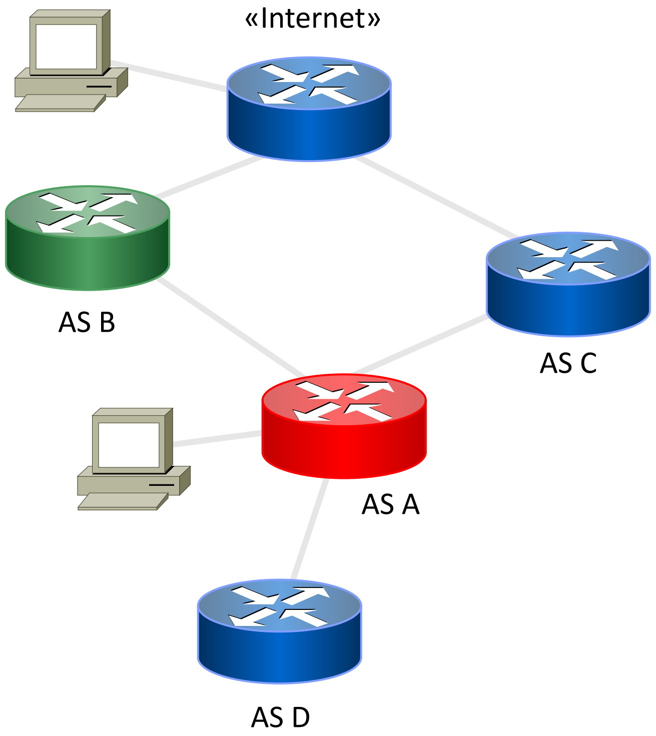
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network



Anti-Spoofing

For each Provider:

Gather

Parse

Analyze

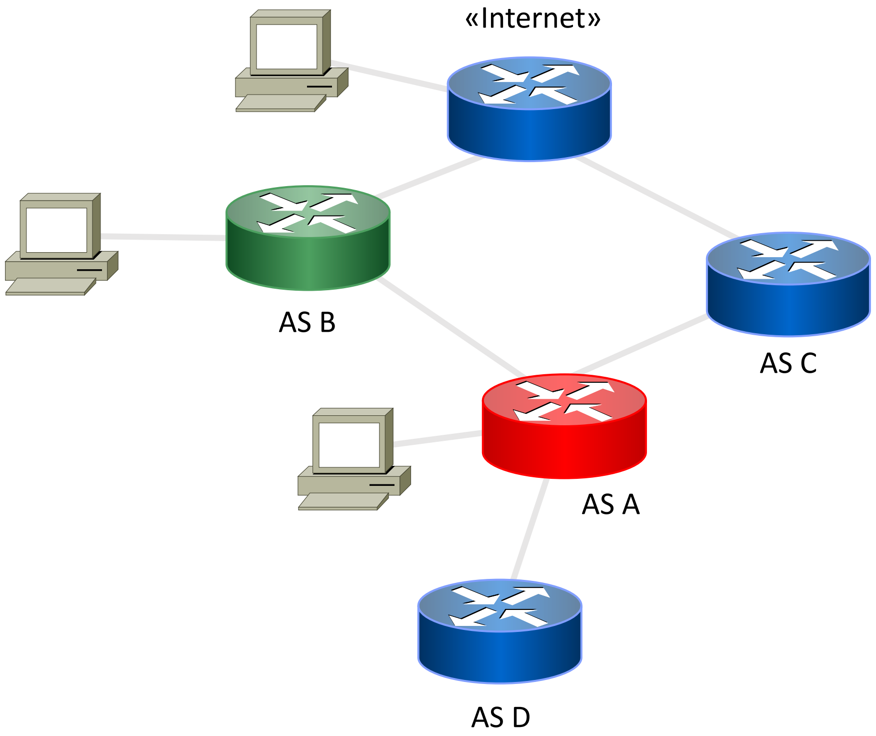
Emulate

ROSE-T – Step-by-Step

Routing Security Tool

Verify "Anti-Spoofing" and "Filtering"

On the Emulated Network



Anti-Spoofing

For each Provider:

1. Insert a Client

Gather

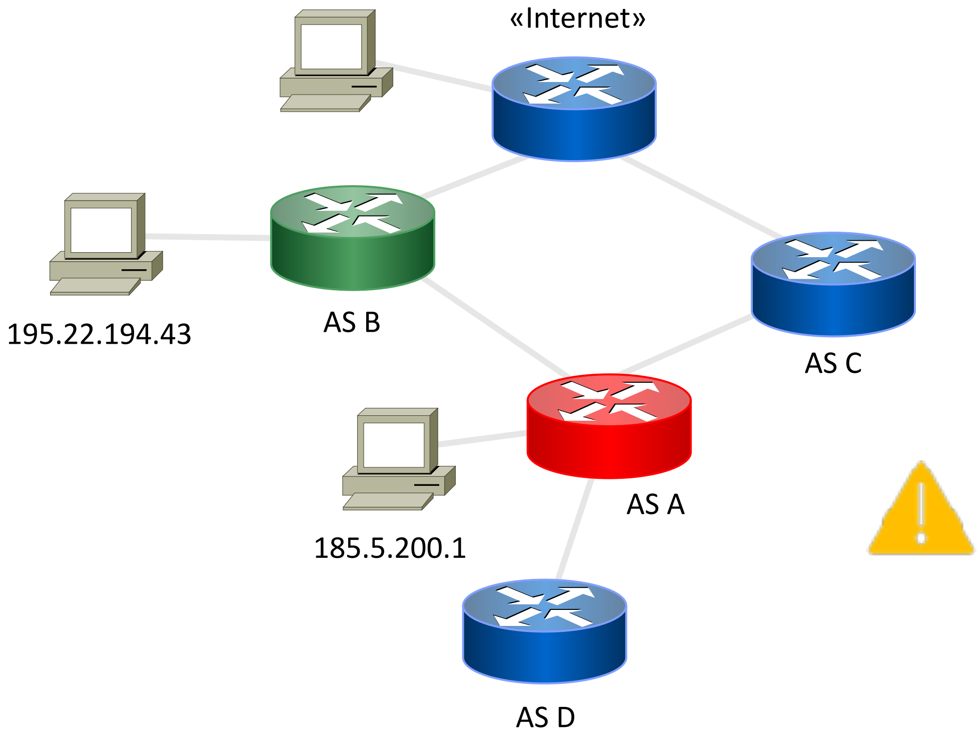
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

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

⚠ Carefully choose subnets that are correctly announced and reachable

Gather

Parse

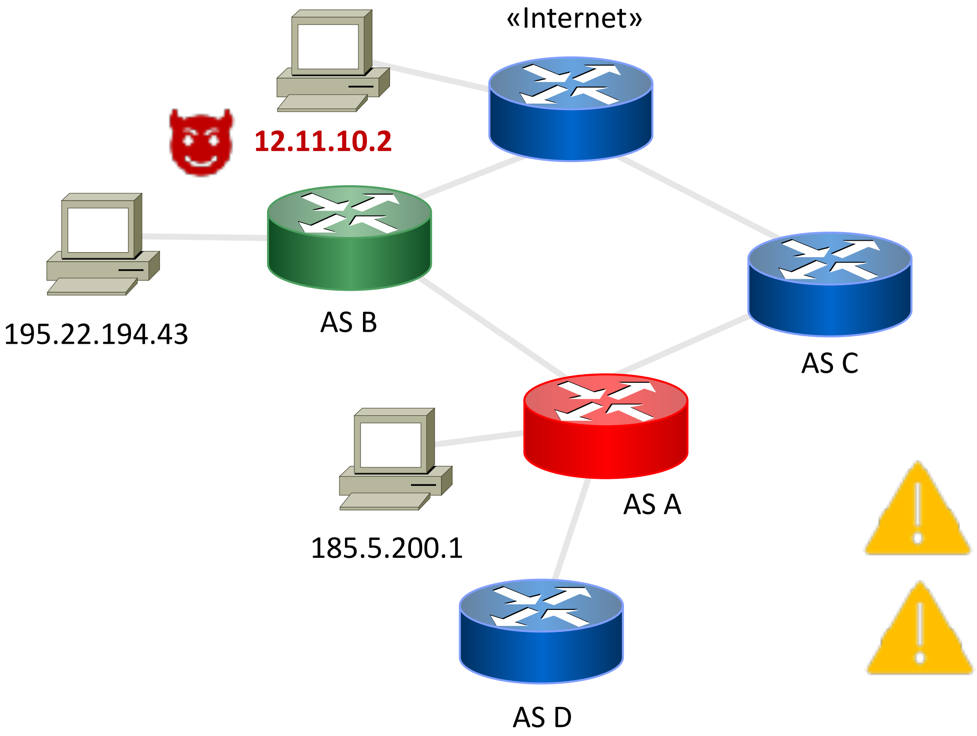
Analyze

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

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

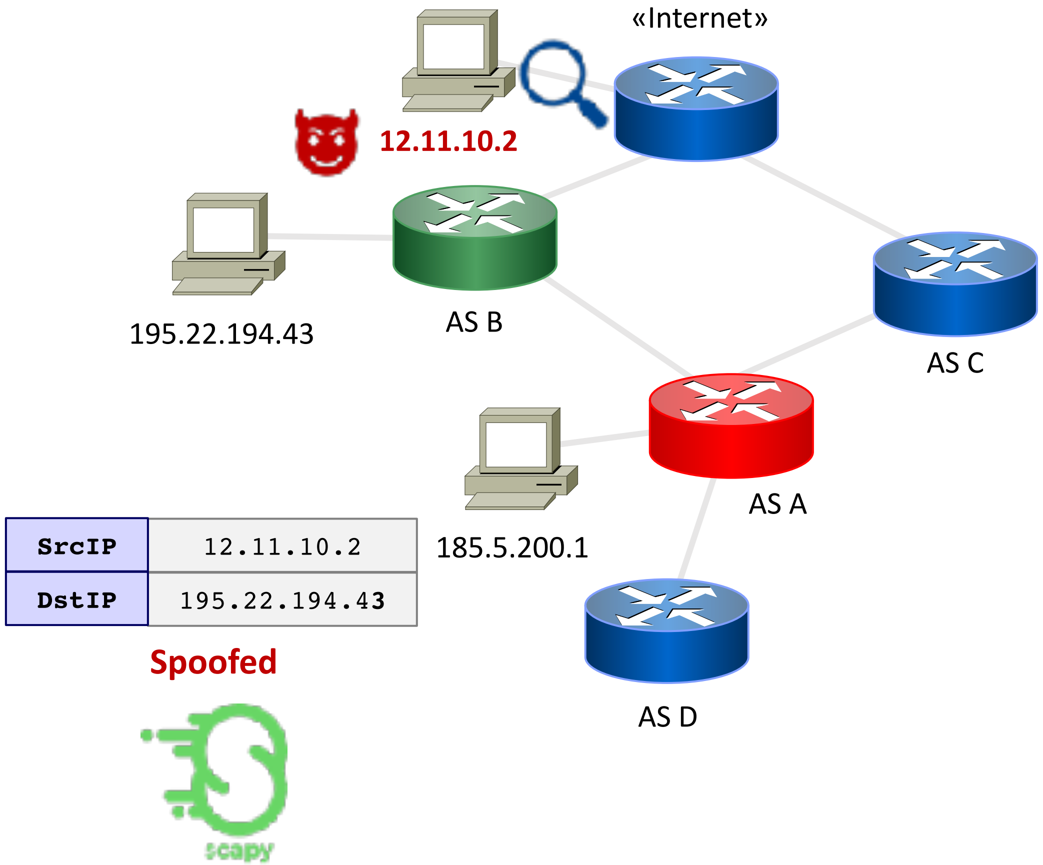
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

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

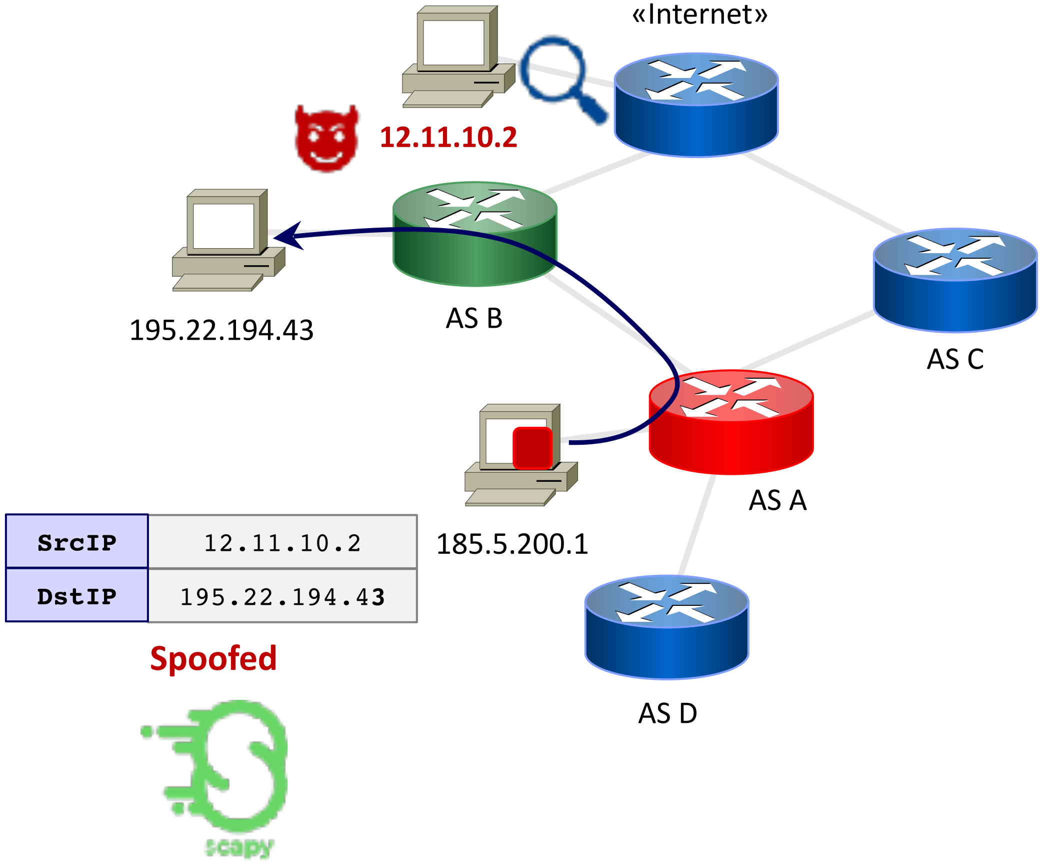
Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network



SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

Anti-Spoofing

For each Provider:

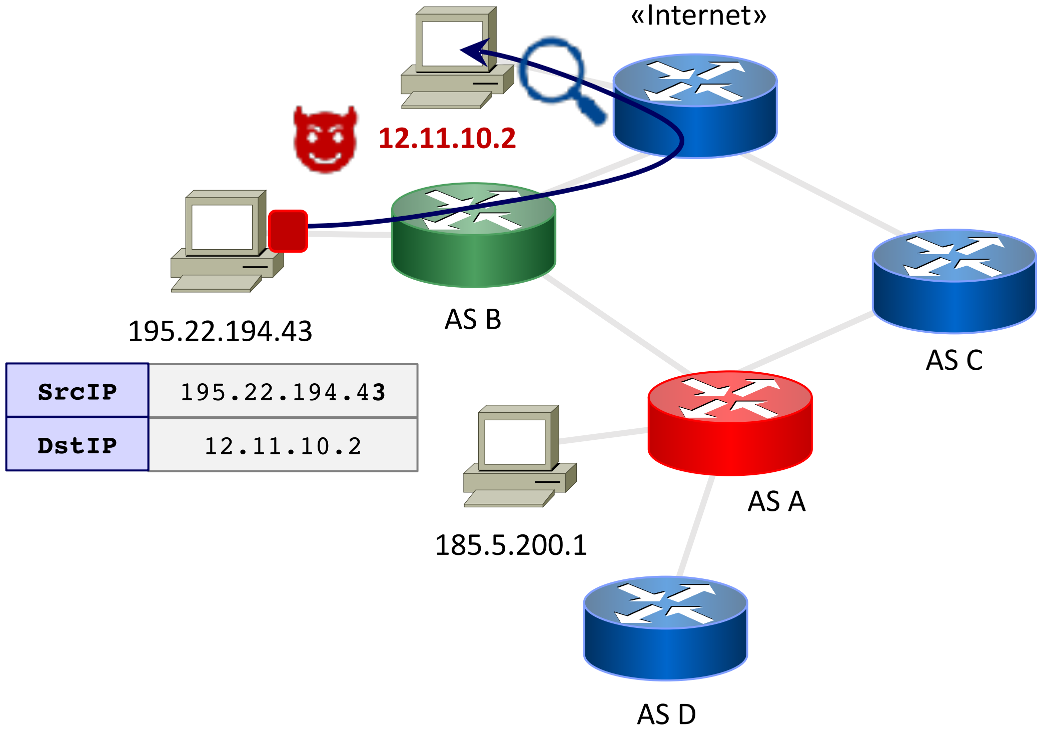
1. Insert a Client
2. Assign IPs (v4/v6) to each Client
3. Send the spoofed ICMP packet

- Gather
- Parse
- Analyze
- Emulate

ROSE-T – Step-by-Step

Routing Security Tool
Rose-T

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



SrcIP	195.22.194.43
DstIP	12.11.10.2

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

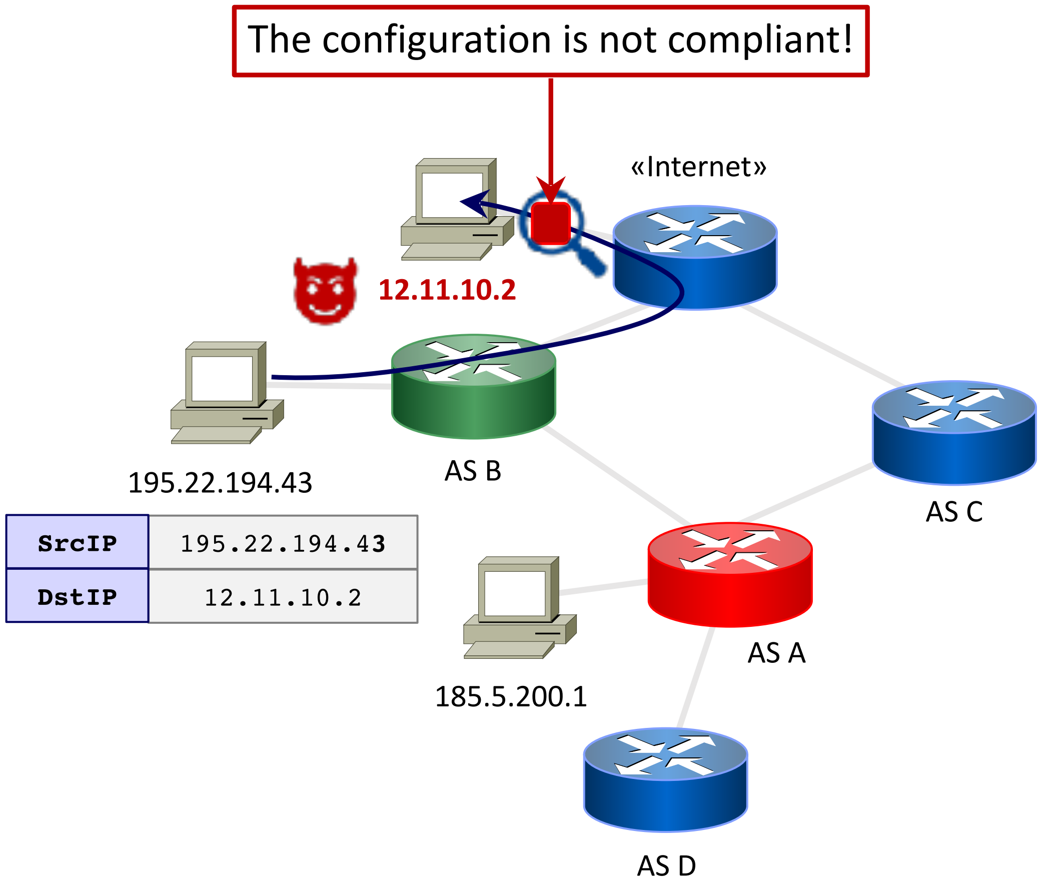
Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network


The configuration is not compliant!

SrcIP	195.22.194.43
DstIP	12.11.10.2

Anti-Spoofing

For each Provider:

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

Gather

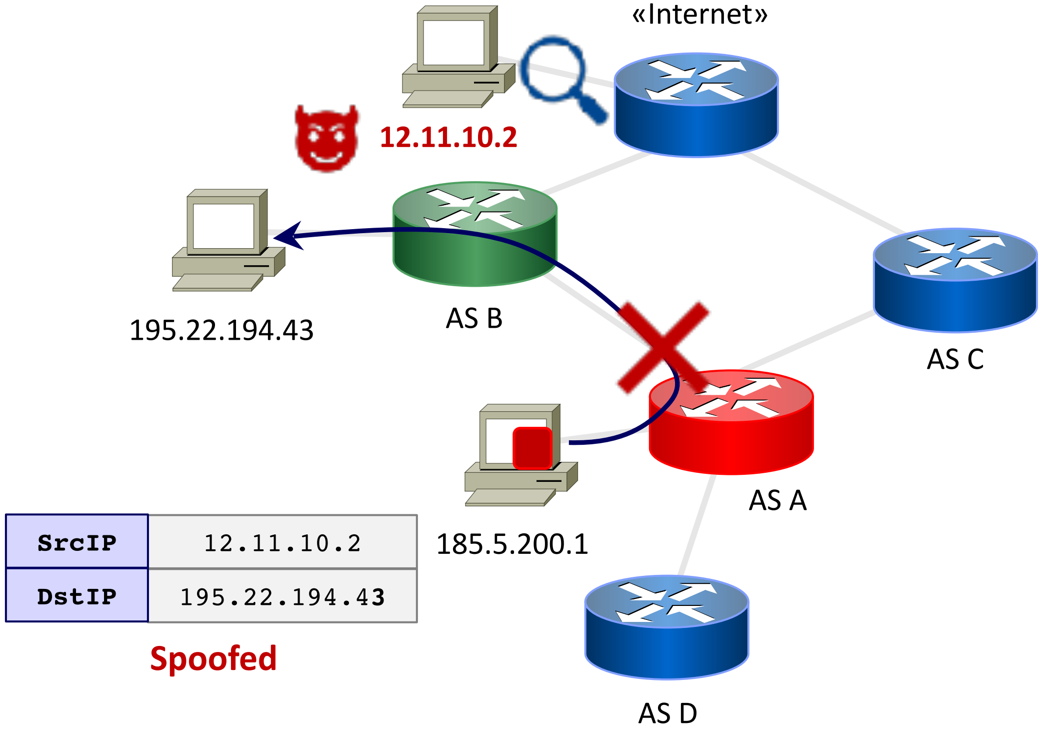
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

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



SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

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

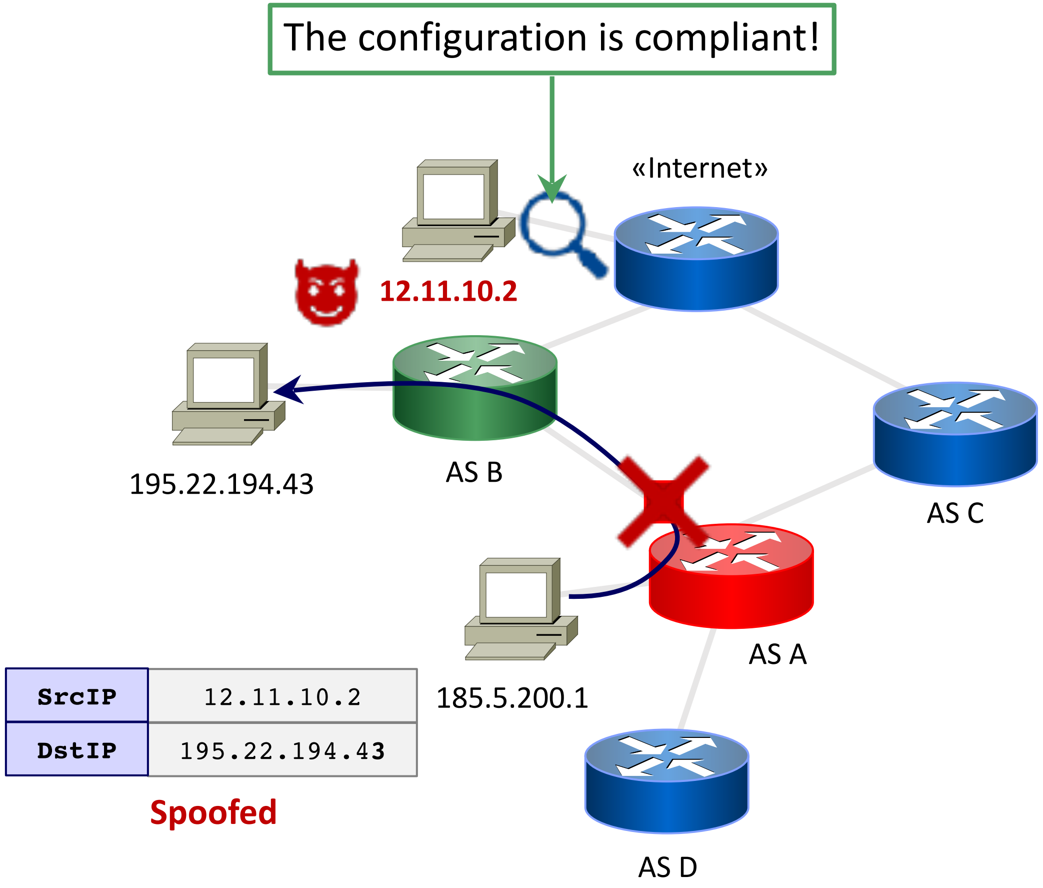
Analyze

Emulate

ROSE-T – Step-by-Step

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network


The configuration is compliant!

SrcIP	12.11.10.2
DstIP	195.22.194.43

Spoofed

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

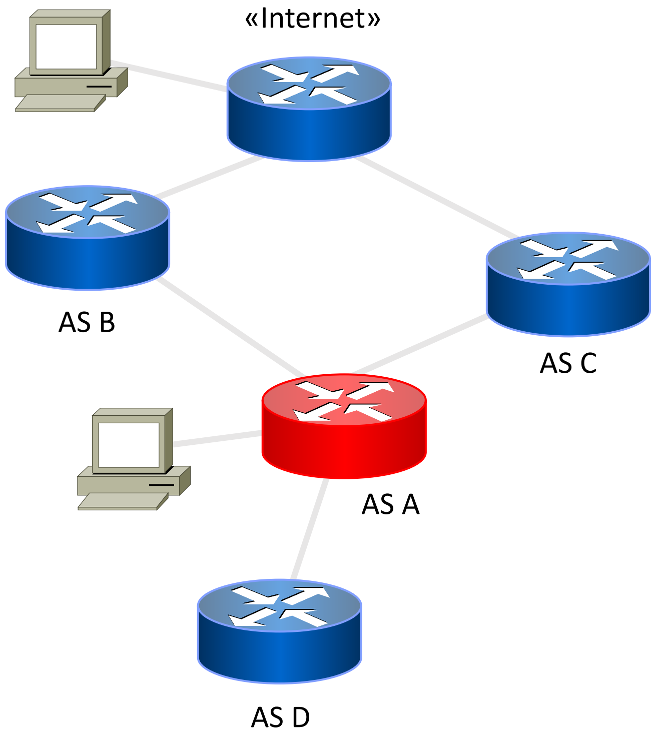
Analyze

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

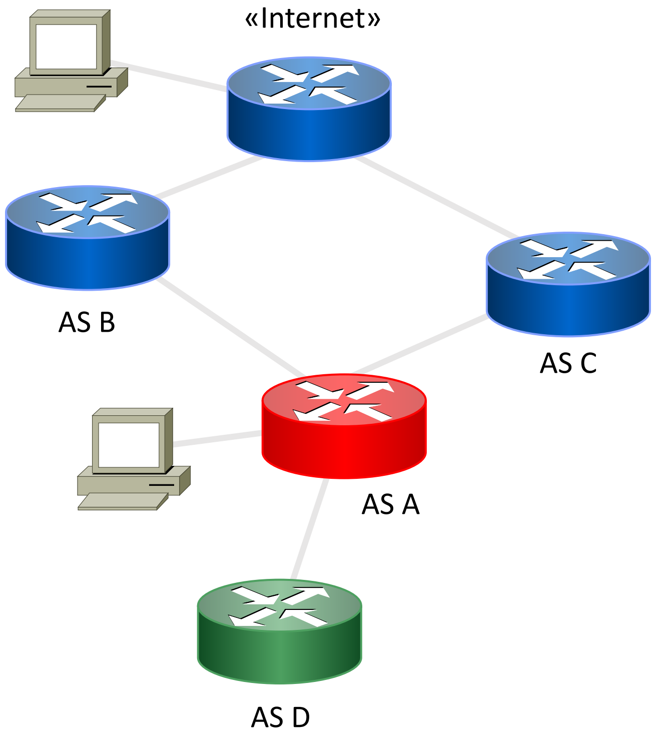
ROSE-T – Step-by-Step

Routing Security Tool

Rose-T

Verify “Anti-Spoofing” and “Filtering”

On the Emulated Network



Filtering

For each Customer:

Gather

Parse

Analyze

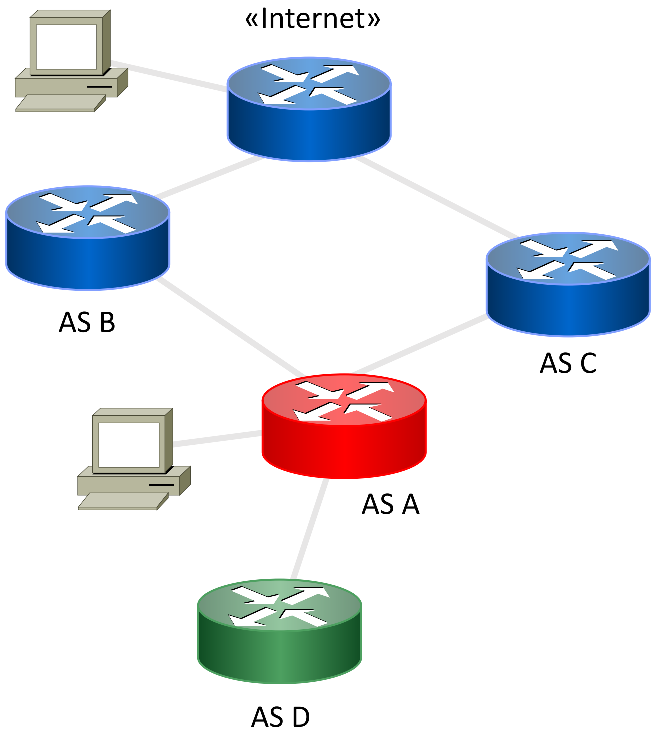
Emulate

ROSE-T – Step-by-Step

Routing Security Tool

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

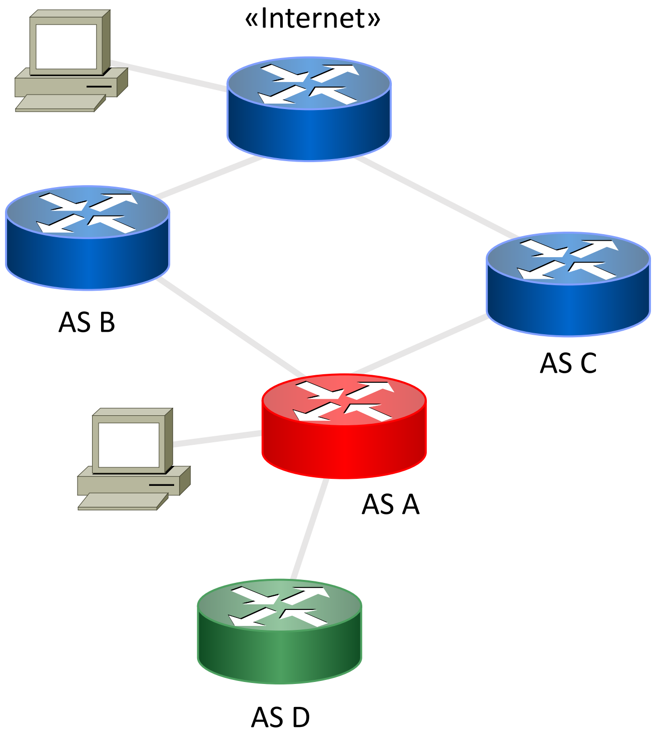
Emulate

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

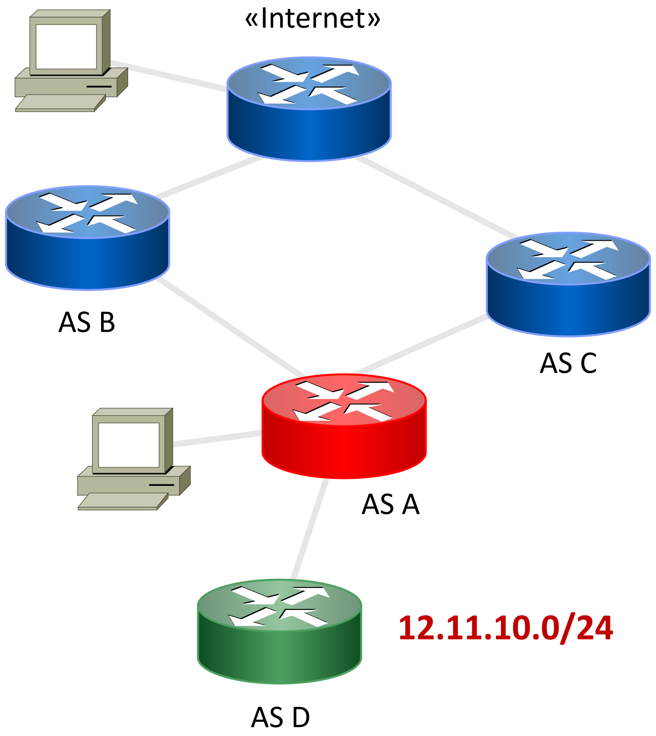
Analyze

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

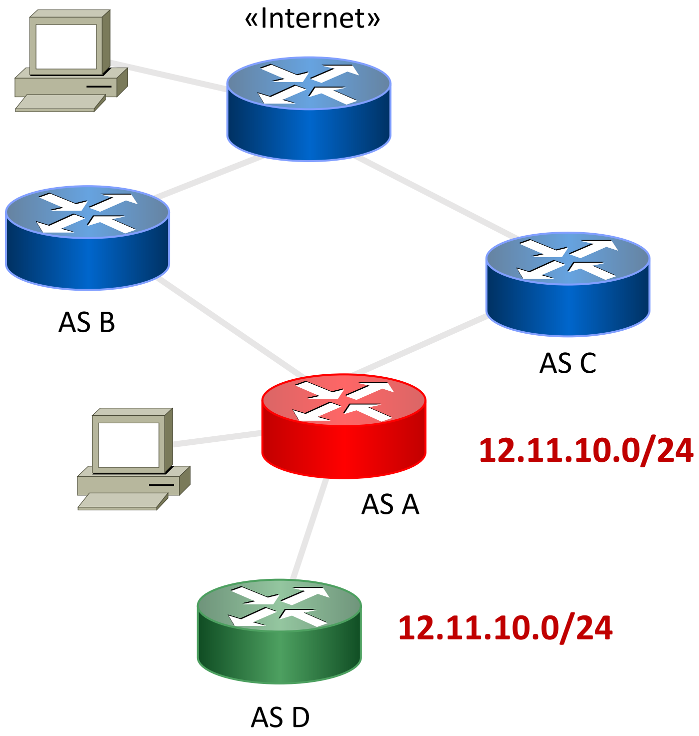
Parse

Analyze

Emulate

ROSE-T – Step-by-Step

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

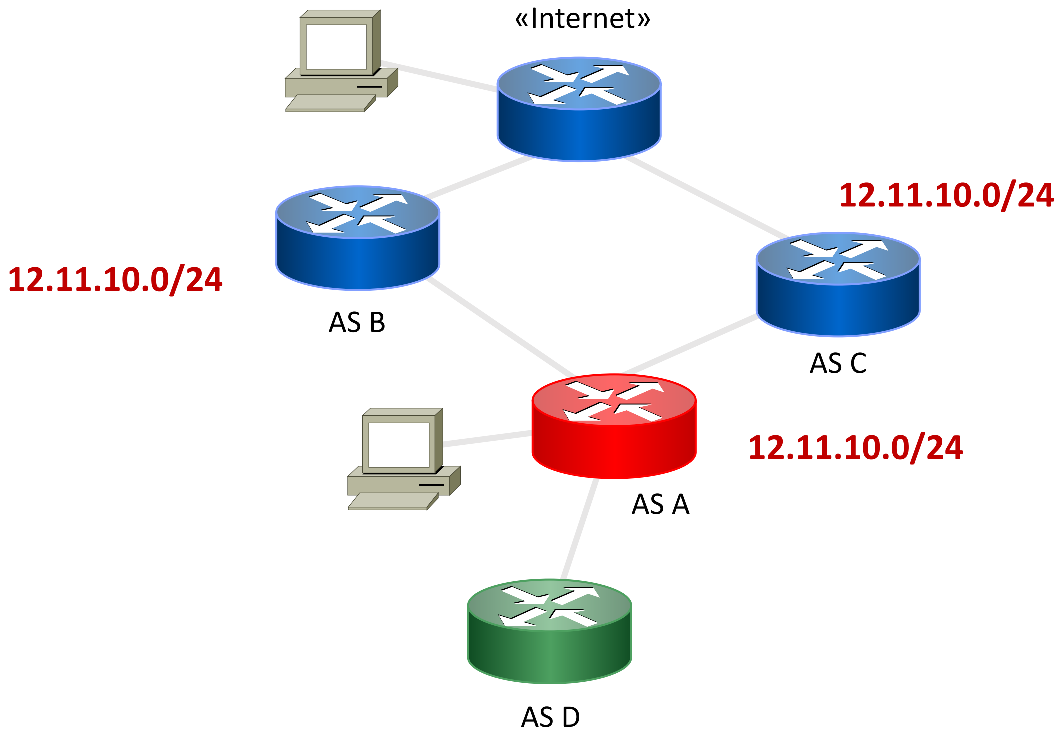
Emulate

ROSE-T – Step-by-Step

Routing Security Tool

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

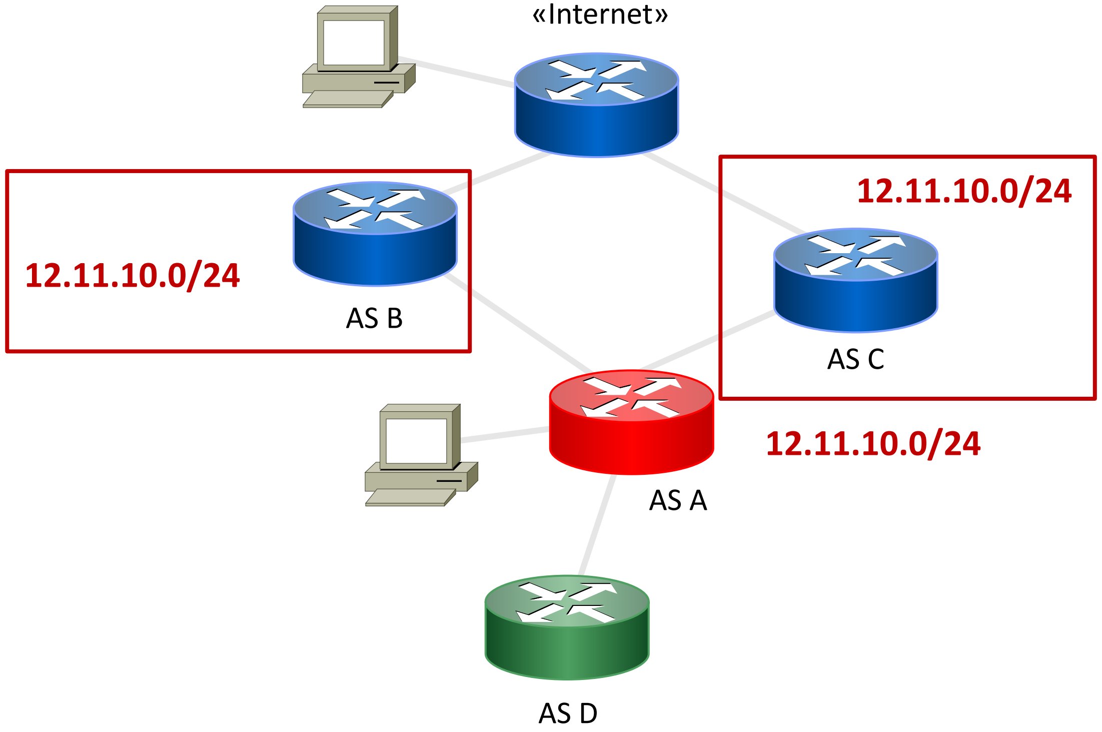
Emulate

ROSE-T – Step-by-Step

Routing Security Tool

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

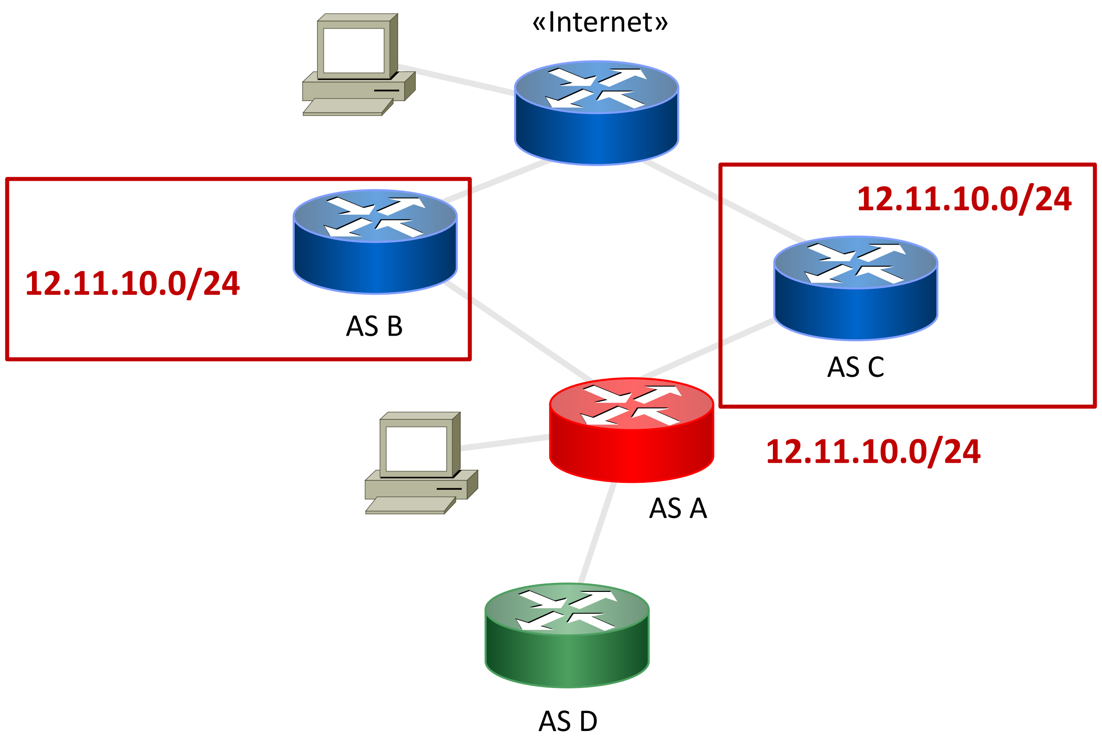
Analyze

Emulate

ROSE-T – Step-by-Step

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

The configuration is not 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

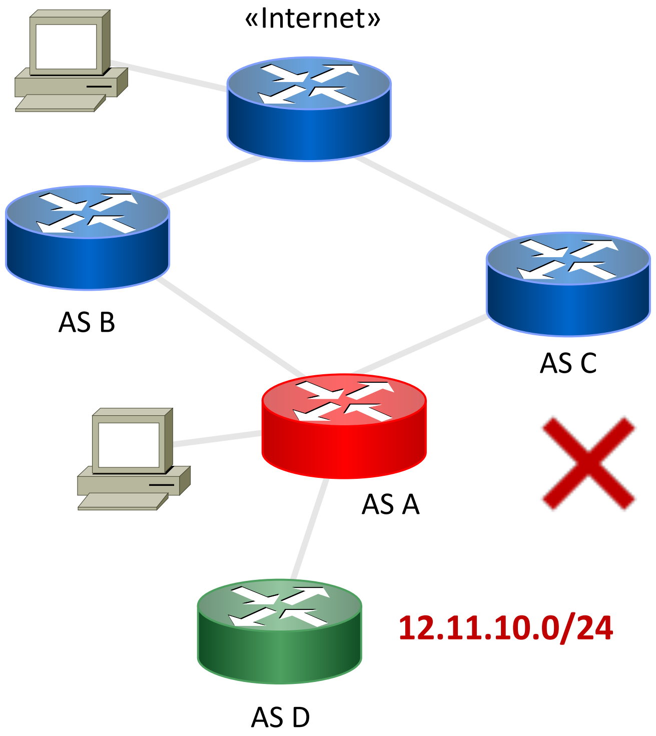
Analyze

Emulate

ROSE-T – 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

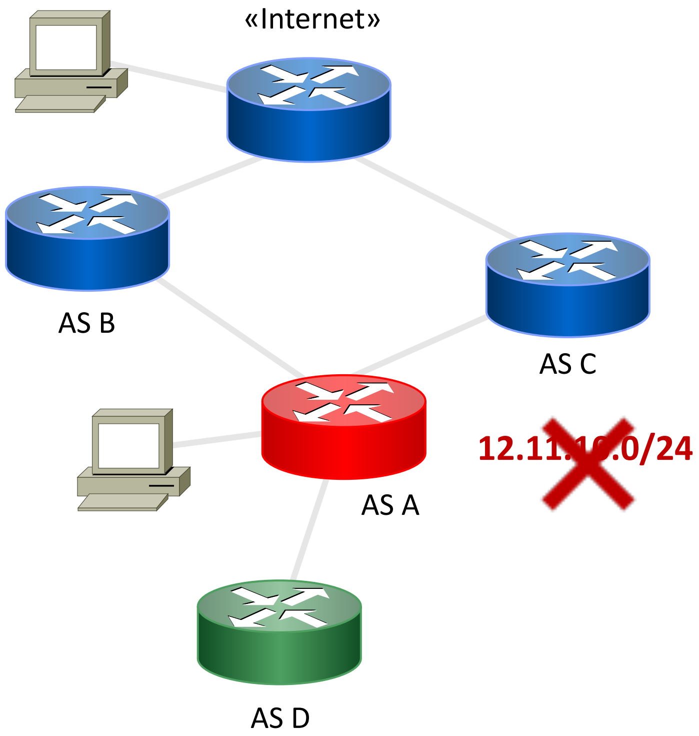
Emulate

ROSE-T – Step-by-Step

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

Conclusions

The **ROSE-T** tool:

- Implements the **first tool** to **automatically** verify MANRS compliance
- Allows network operators to test their configurations without relying on **manual and error-prone** procedures
- **Reduces the time** for MANRS adoption that would lead to a **more secure** global routing infrastructure

Future Work

- Support to verify multiple routers' configuration compliance (on going)

- Currently, ROSE-T implements the verification of Network Operators Actions
  - Expand the support to IXPs and CDNs Verification

- ROSE-T aims to verify networks beyond MANRS…
  - MANRS+
  - Emulate the RPKI infrastructure
  - Additional features (*e.g.,* ASPA validation)

- Web UI to perform the validation process

Contacts

Mariano Scazzariello

KTH Royal Institute of Technology

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!