This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 643964.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0091.

Resilient Multi-Cloud Virtual Networks
Jan 2018

Max Alaluna, Eric Vial, Fernando Ramos, Nuno Neves
LASIGE, Faculdade de Ciências da Univ. de Lisboa

User-centric management of security and dependability in clouds of clouds
Overview of Sirius
Building a *Substrate Network*
Machine Virtualization Support
Containers Support
Building a *Substrate Network*

Data Center
User-centric management of security and dependability in clouds of clouds

Private Cloud
Multi-cloud Network Substrate that encompasses a diverse set of resources
Define an arbitrarily large application

Deploy over the substrate network

Public Cloud 1

Public Cloud 2

Private Cloud
Building Virtual Networks

Define an arbitrarily group of applications

VNs are deployed dynamically, effectively sharing the resources

Ensure "complete" network virtualization

Application A (or virtual network A)

Application B (or virtual network B)

Application C (virtual network C)

Public Cloud 1

Public Cloud 2

Private Cloud

13 January, 2018

User-centric management of security and dependability in clouds of clouds

11
Adding Multi-Cloud Storage

Private Cloud

Application A (or virtual network A)

Public Cloud 1

Application B (or virtual network B)

Public Cloud 2

Application C (virtual network C)

Storage Services of Cloud Providers

CHARON

User-centric management of security and dependability in clouds of clouds
Sirius

SECURE AND DEPENDABLE
MULTI-CLOUD NETWORK VIRTUALIZATION
Characteristics of existing platforms

- Target: single-cloud
  - Single operator, single provider

- Networking services: traditional
  - flat L2
  - L3 routing
  - ACL filtering
Our goal

• Target: **multi-cloud**
  ◦ Public clouds + private datacenters

• Networking services
  ◦ flat L2, L3 routing, ACL filtering
  ◦ **security & dependability needs over virtual resources**

• Benefits
  ◦ **Scalability**: scale out the network to accommodate growth; support large numbers of VNRs/sec; allow for large VNs
  ◦ **Performance**: leverage from locality to bring services nearer to customers
  ◦ **Security**: explore clouds with different security assurances; contribute to ensure privacy regulations
  ◦ **Dependability**: replicate services, either in the same cloud or distinct clouds
Multi-Cloud Orchestrator

Network Hypervisor
SDN controller

Sirius architecture

Cloud provider 1

Public cloud
VM manager

GRE TUNNEL

OvS

Container Hypervisor

Secure Tunnel

Private datacenter
VM manager

OvS

GATEWAY

OvS

GATEWAY

OvS

GRE TUNNEL

GRE TUNNEL

GRE TUNNEL

Private cloud

Cloud provider 2
Orchestrator: Main software modules

**Multi-cloud Orchestrator**

- Manage interactions with users, namely setup & status update of the substrate and the specification of VNs

- Hypervisor Support
  - VM config & bootstrap
  - Network Updates

- User & Cloud Manager
  - Topology inform
  - Virtual Network
  - User GUI

- Topology
  - Topology inform

- Multi-cloud Provision
  - Admin GUI
  - Public & Private Cloud VMs

- Network Hypervisor
  - VM & Container Storage

Bootstraps and configures VMs in the clouds, setting up the tunnels; starts the containers of the VNs together with the hypervisor

Keep information about substrate topology and VN mappings
Inter- and intra-cloud connections

Gateway acts as an edge router, interconnecting the various clouds

Local VMs run the tenants’ containers, enforcing isolation of the communications

Public IPs that work as endpoints of secure tunnels (openVPN) between clouds

GRE tunnels interconnect the local VMs within a cloud, which have private (local) IPs
Finds a mapping onto the substrate after the arrival of a VNR, taking into consideration the constraints of the substrate and requirements of the user.

Keeps information about substrate, by interacting with orchestrator and switches.

Maintains information about VNs, and finds appropriate paths in the network.

Implemented as a module of the SDN controller, setting up the flow tables, monitoring the network and ensuring isolation.
Secure and Dependable Network Embedding
Overview of the Embedding

Virtual Networks

Substrate Network

Virtual host
Virtual edge switch
Virtual transit switch

Substrate compute
Inter-cloud tunnel
Intra-cloud tunnel
Substrate soft switch
Substrate fabric switch
Substrate link

13 January 2018
User-centric management of security and dependability in clouds of clouds
A node in the model corresponds to an entity capable of forwarding decisions. A node at the edge aggregates the requested resources, namely the CPU is the sum of the needs of the virtual edge switch plus all connected virtual hosts.

A virtual transit switch is directly modeled by a node with equivalent requirements.

Similar approach is followed for the maximum bandwidth & latency of the virtual links. Likewise, for the substrate network the model captures the available components and resources.
Sec & Dep Controls:

Firewall
IDS & IPS
DPI
VM introspection
Secure tunnels
DoS protection
Monitoring
Traffic shaping
Traffic engineering
Encrypted file system
Replication
...

1) Applied at the infrastructure level
but the user has little control in public clouds
Sec and Dep Attributes

Amazon Cloud

Last Updated: December 2016

This Amazon Compute Services (APS) Customer Agreement (the "Agreement") is between Amazon’s Datacentre Operations ("us" or "we") and you. The terms will have the meaning as set forth in this SLA in accordance with its terms.

Included Products

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Block Storage (Amazon EBS)
- Amazon Elastic Content Delivery Network (Amazon CloudFront)
- AWS Fargate for Amazon ECS (AWS Fargate)

Amazon launches new cloud storage service for U.S. spy agencies

By Aaron Gregg  November 20, 2017

Amazon’s cloud storage unit announced Monday that it is releasing a new service called the Amazon Web Services Secret Region, a cloud storage service designed to handle classified information for U.S. spy agencies.

but the user has little control in public clouds

User-centric management of security and dependability in clouds of clouds
Sec and Dep Attributes

Sec & Dep Controls:
- Firewall
- IDS & IPS
- DPI
- VM introspection
- Secure tunnels
- DoS protection
- Monitoring
- Traffic shaping
- Traffic engineering
- Encrypted file system
- Replication
- ...

1) Applied at the infrastructure level, **but** the user has little control in public clouds

2) Applied in the containers, where the user has full control, **but** it is outside the scope of Sirius

3) Applied in the VMs or Container Manager, where the user can either acquire or setup more secure solutions,

nothing is done

associate a numeric Trust Level to the cloud

13 January, 2018
User-centric management of security and dependability in clouds of clouds
Sec and Dep Attributes

Trend Micro Deep Security

(1) | Version Deep Security 10.2 | Sold by Trend Micro

Security built to fit DevOps with robust API's and automated protection. Lock down servers with Application Control, protect Docker containers, and increase malware protection...

Azure Marketplace

Barracuda NextGen Firewall F-Series

By Barracuda Networks, Inc.

CloudLink SecureVM by Dell EMC

By Dell EMC

Control, monitor and encrypt VMs with ease and confidence

HP Security Fortify Application Defender

By HPE Security Fortify Application Defender Agent

Lacework

Lacework security solutions deploy to protect against emerging threats.

VM-Security

Free Trial

Sec & Dep Controls:

- Firewall
- IDS & IPS
- DPI
- VM introspection
- Secure tunnels
- DoS protection
- Monitoring
- Traffic shaping
- Traffic engineering
- Encrypted file system
- Replication

1) Applied at the infrastructure level but the user has little control in public clouds

2) Applied in the containers, where the user has full control, but it is outside the scope of Sirius; nothing is done

3) Applied in the VMs or Container Manager, where the user can either acquire or setup more secure solutions, associate a numeric Trust Level to the cloud
Sec & Dep Controls:
Firewall
IDS & IPS
DPI
VM introspection
Secure tunnels
DoS protection
Monitoring
Traffic shaping
Traffic engineering
Encrypted file system
Replication
...

1) Applied at the infrastructure level
but the user has little control in public clouds

2) Applied in the containers, where the user has full control, but it is outside the scope of Sirius

3) Applied in the VMs or Container Manager, where the user can either acquire or setup more secure solutions, but there is an extremely large number of combinations controls

associate a numeric
Security Level
and allow for an indication of
Availability Level

nothing is done

associate a numeric
Trust Level to the cloud

13 January, 2018
User-centric management of security and dependability in clouds of clouds
Modeling: (Cloud) Trust Level

Virtual Networks

Substrate Network

Cloud Trust Levels

Public Cloud

Trusted Public Cloud

Highly Trusted Private Cloud
Guidelines for the design

- Optimal embedding solutions, for example, based on solving linear program optimizations do not scale => resort to a greedy approach with utility functions to guide selection

- Mapping of virtual resources to the substrate carried out in two phases, where in the first nodes are embedded and then the links

- Normal resources are mapped first and then the backup resources allocated, giving precedence to the more common failure-free executions
Embedding Nodes

Virtual network

Higher for nodes requiring
- more CPU & bandwidth
- less security & cloud trust

Substrate network

Higher for nodes with
- more residual CPU & bandwidth
- less sec & cloud trust
- fewer hops away from subst. nodes already used to provision neighbors

NScore(n^V)

Order of processing

UPath(n^S, n^V)

Order of processing

Map nodes sequentially

Choose nodes with enough sec and cloud trust, avoid nodes already picked
Find $k$-edge disjoint shortest path between nodes & choose up to MaxP paths that ensure latency. Distribute load through them.

Remove edges not sufficiently secure.

Map each edge sequentially.
Backup nodes and links

- Use similar algorithms to reserve resources for the nodes that have requested backups
- Reserve appropriate paths to connect them together and to the normal nodes
- Avoid selecting the same substrate nodes and edges to prevent common failures
  - Exceptions have to exist in case substrate does not encompass a sufficient level of redundancy (e.g., ToR switches)
Approaches under consideration

- Sirius with Path Contraction *(FOO)*
- Sirius without Path Contraction *(FOO w/o PC)*
- Sirius with Multi-Commodity Flow (MCF) & w/o PC *(FOO wMCF)*
- D-Vine by Chowdhury et al. *(DVINE)*
  - relaxation of a MIP for node mapping & MCF for link mapping
- Full Greedy by Yu et al. *(FG)*
  - greedy approach for node mapping & MCF for link mapping
- Full Greedy with Shortest Path *(FG+SP)*
• Simulations
  ◆ Simulator of online VNR embedding
  ◆ Substrate
    ▪ Public clouds with a Waxman topology (50% link prob.)
    ▪ Private cloud with Google's Jupiter topology
    ▪ Substrate nodes & links with different characteristics
  ◆ VNRs with various requirements, namely about sec & avail

• Real testbed
  ◆ Substrate composed of Amazon & Google & FCUL
Notation | Requirements of the generated VNRs
--- | ---
NS+NA | no security or availability demands on the VNRs
10S+NA | VNRs with 10% of resources (nodes and links) with security demands (excluding availability)
20S+NA | like 10S+NA, but with security demands for 20% of the resources
NS+10A | VNRs with no security demands, except for 10% of the nodes requesting replication
NS+20A | like NS+10A, but for 20% of the nodes
20S+20A | 20% of the resources (nodes and links) with security demands and 20% of the nodes with replication
Multi-commodity flow & DVINE do not scale to large networks

Private Cloud: CLOS-based topology
Substrate (1900 nodes); VNRs (40-120 nodes)

Sirius can achieve a higher acceptance ratio than full-greedy for NoSecAvail, and even with Sec requirements

Multi-Cloud: 3 PublicCl + 1 PrivateCl
Substrate (2500 nodes); VNRs (40-120 nodes)
Even in comparatively small networks

- **DVINE** is 4 orders of magnitude slower for node mapping
- Multi-commodity flow is 2 orders of magnitude slower than shortest path
Link Embedding at Large

**Link mapping in the order of 1 min for considerably large networks**

![Graph showing Link Embedding Time]

- **Link Embedding Time**
- Substrate (2500 nodes); VNRs (40-120 nodes)

**Time of Working Link Mapping (ms)**

- FOO
- FOO (w/oPC)
- FG+SP

- NS+NA
- 20S+NA
- NS+20A
- 10S+NA
- NS+10A
- 20S+20A

13 January, 2018

User-centric management of security and dependability in clouds of clouds
(Very Rough Estimate) Revenue & Link Costs

Sec & Dep services can improve revenue because of added value

Revenue: Proportional to the quantity & price of sold resources
Substrate (100 nodes) and VNRs (5-20 nodes)

Cost: Total number of allocated substrate links
Substrate (1900 nodes) and VNRs (40-120 nodes)

Path Contraction can decrease noticeably the number of allocated substrate links
Substrate creation time is significantly affected by VM configuration times (e.g., Docker installation, get basic container ...)

- VN embedding calculation is about 1%
- 10K container VN takes around 4 min
Sirius allows the setup of a **rich** substrate environment, with public/private cloud resources, **supporting** the deployment of virtual networks with security and dependability requirements.

Our VNE solution achieves all requirements set:

1. **scales** to very large virtual networks, as a node can connect 1000 containers with ease.
2. **increases the acceptance ratio** and the provider profit for diverse topologies.
3. **maintains short path lengths**, enhancing application performance and decreasing provider costs.
SUPERCLOUD Grant Agreement No. 643964

"The project SUPERCLOUD has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 643964."

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55    Fax: +43 4242 233 55 77
E-Mail: coordination@supercloud-project.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.