Secure Inter-Cloud Architecture for Virtual Cloud Computing Based on Hybrid IP and MPLS Infrastructure Solution

A. Boava and Y. Iano

***Abstract*— The Next Generation Networks use MPLS protocol in the core network to provide new services that are based on MPLS IP Cloud. This article describes an evaluation of key aspects for the construction of security on MPLS IP Inter-Cloud. The aspects to be evaluated are: separation of traffic between users of MPLS Inter-Cloud, connectivity among sites of the same Cloud application, protection of core of the cloud provider and possibility of using the same plan addresses by users, provided that they are in different MPLS IP Cloud. To achieve this goal it was proposed an architecture for assessment test.**

***Keywords*— Cloud, MPLS, Security, Inter-Cloud, Internet Protocol.**

I. INTRODUÇÃO

CONFORME [13], a computação em nuvens é uma tecnologia que fornece aos usuários capacidade de processamento, armazenamento de dados e aplicações via rede, através de um modelo de computação utilitária [6], onde recursos computacionais e software são oferecidos como serviços e pagos por uso (pay per use). Ela fornece aos seus consumidores acesso a recursos computacionais que não estariam disponíveis em arquiteturas tradicionais, devido à complexidade técnica e aos altos custos envolvidos [10]. Mesmo com os grandes investimentos feitos na área de segurança em nuvens, a segurança ao lado da qualidade de serviço são considerados os maiores fatores impeditivos para motivar a migração dos usuários dos serviços legados para um ambiente em nuvem.

De acordo com [8], os ambientes de nuvens atuais apresentam centenas de nuvens independentes e heterogêneas, mas muitos provedores de nuvens já demandam a necessidade de uma nova arquitetura de rede que possibilite as interconexões das nuvens (Inter-Cloud). Ao identificar a segurança como uma das principais preocupações para o provedor, o autor propõe um modelo funcional de gerenciamento para a segurança Inter-Cloud que permite a identificação, integração e gestão das funções de segurança.

Em [1] é feito uma análise detalhada dos problemas de segurança em nuvem. Os problemas de diferentes sistemas de computação em nuvem e o efeito sobre os usuários são analisados. A solução proposta pelo autor é baseada principalmente no uso de sistema de criptografia de chave pública e privada.

A. Boava, Universidade Federal de Santa Catarina (UFSC), Florianópolis, Brasil, adao.boava@ufsc.br

Y. Iano, Universidade Estadual de Campinas (Unicamp), Campinas, São Paulo, Brasil, yuzo@decom.fee.unicamp.br

Com o objetivo de contribuir para o desenvolvimento de uma arquitetura de nuvens seguras e com alto desempenho, o maior desafio dos provedores de serviços de nuvens é encontrar uma alternativa com um protocolo que considere os vários riscos de segurança para que possam motivar a migração das arquiteturas tradicionais dos usuários para o ambiente de nuvens. Nesse contexto o correto entendimento desses protocolos que interferem nas topologias é de relevante importância. Sob essa ótica, uma nova arquitetura de nuvens computacionais segura é, em si, o desejo de todos os provedores de nuvens e dos usuários. Para ser possível propor uma alternativa para os ambientes de computação em nuvem é fundamental que se avalie em detalhes os possíveis padrões de segurança para as nuvens para em seguida investigar uma nova proposta de arquitetura computacional para as nuvens computacionais baseadas nos protocolos IP e MPLS. Conhecendo os riscos das nuvens e as tecnologias de redes IP baseadas no protocolo MPLS, será possível propor uma nova arquitetura e construir cenários reais para realizar os testes e validar a nova arquitetura proposta.

A solução proposta utilizando o MPLS transfere para o provedor todos os aspectos relacionados à segurança das interconexões das nuvens e possibilita aos usuários a visão de somente uma nuvem, deixando transparente para os usuários as interconexões de várias nuvens. Uma proposta de nuvem baseada em MPLS tem a capacidade de interconectar várias nuvens internas e externas proporcionando interoperabilidade entre as nuvens de forma transparente ao usuário do serviço. As nuvens baseadas em MPLS oferecem ao provedor de nuvens uma nova plataforma de nuvem altamente escalável e com custo independente da localização geográfica e da topologia da rede do usuário.

A crescente preocupação e insatisfação com a segurança em serviços de nuvens é resultado de uma combinação de diversos fatores, dentre os quais podem ser citados: a falta de conhecimento das características técnicas e riscos existentes em ambientes de nuvem [6, 13]; a falta de padrões de interoperabilidade bem definidos [2]; a perda de controle de dados e aplicações [11]; as falhas ocorridas em nuvens computacionais que resultaram em indisponibilidade de serviços, perda de dados e vazamento de informações [15]; e a falta de garantias relacionadas ao nível de segurança [3].

Diante desses problemas, percebe-se a necessidade de um modelo não apenas de interconectividade entre nuvens de forma segura, mas também que permita que usuários de diferentes nuvens não acessem indevidamente usuários de outras nuvens e que faça o isolamento entre nuvens devidamente. Entre os principais requisitos das internuvens

(inter-cloud) para atender às necessidades das novas aplicações em relação à segurança, podemos destacar:

A. Separação/Isolamento de tráfego das Nuvens MPLS

Um dos requisitos de segurança mais importantes das nuvens é que a rede não deve permitir que o tráfego de um usuário de uma determinada nuvem seja visto, nem que invada o tráfego da outra nuvem. A avaliação de desempenho realizada nesse artigo mostra a eficiência da nova proposta das nuvens baseadas em MPLS em relação a esse requisito.

B. Utilização do mesmo plano de endereços por diferentes nuvens

Outro requisito importante para um provedor que as novas tecnologias de nuvens devem oferecer é permitir que o plano de endereçamento de um usuário de uma nuvem possa ser utilizado por outra nuvem, sem afetar outras nuvens ou o núcleo da rede. A nova arquitetura proposta apresenta uma boa alternativa para esse requisito, que serão avaliados durante o teste da nova arquitetura baseada em MPLS. Em outras palavras, uma dada nuvem deve ser completamente separada das outras nuvens ou do núcleo da rede em termos do tráfego ou plano de endereços. Para tornar possível utilizar o mesmo plano de endereços IPs para vários usuários, a nova arquitetura utiliza o campo RD (***Route Distinguisher***) para distinguir as nuvens entre si.

Basicamente temos dois modelos de implementação de modelo em nuvens: O inter-cloud e a federação em nuvens. O termo inter-cloud foi introduzido pela Cisco e se refere a uma malha de nuvens interligadas para oferecer um ambiente universal de computação em nuvem com base em padrões abertos. Como o nome sugere, é similar ao modelo da Internet, onde tudo é federado em uma infraestrutura ubíqua de múltiplos provedores. A principal diferença entre o intercloud e uma federação de nuvens é que o intercloud é baseado em padrões futuros e interfaces abertas, enquanto a federação utiliza mecanismos específicos de cada fornecedor de serviços. Na visão do intercloud, todas as nuvens deverão ter um entendimento comum de como as aplicações devem ser executadas. Na realidade, essa visão é a percepção da Cisco sobre o mundo IP, como ela foi a responsável pela implementação de IP na grande maioria dos backbones IP das operadoras de telecomunicações, é perfeitamente compreensivo imaginar que ela defenda a proposta de uma única nuvem IP. A Fig. 1[4] apresenta o modelo da arquitetura Inter-cloud [5].

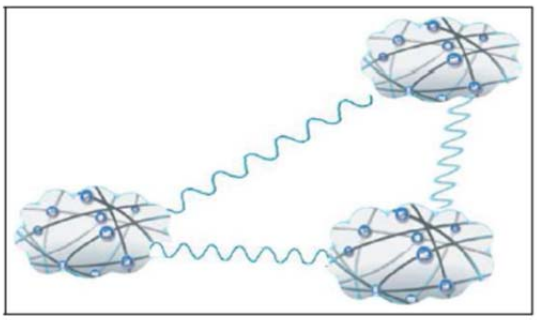

Figura 1. Inter-cloud das nuvens.

Diferente das arquiteturas tradicionais de projetos de nuvens que utiliza o protocolo IP da internet publica como a infraestrutura de suporta a rede, a arquitetura adotada neste artigo é uma solução hibrida com IP e MPLS.

Uma das motivações para aplicar a nova proposta é a limitação de recursos que as operadoras têm como a limitação de números endereços IP, as falhas de segurança dos protocolos da internet publica padrão e os custo de redes das nuvens tradicionais como função geográfica do usuário.

As próximas seções deste artigo estarão organizadas da seguinte maneira: na seção 2 serão abordados os principais conceitos de riscos em computação em nuvem no ambiente das nuvens tradicionais. Na seção 3 será apresentada a nova arquitetura para as nuvens virtuais baseadas em IP MPLS. A seção 4 descreverá os métodos e os testes de conectividade e Isolamento das nuvens IP MPLS. Os resultados dos testes serão apresentados na seção 5 que trata da conectividade e isolamento das nuvens IP MPLS. A seção 6 apresentará a análise dos resultados dos experimentos obtidos. Por fim, na seção 7 estarão as considerações finais.

II. PRINCIPAIS RISCOS EM COMPUTAÇÃO EM NUVEM

Neste artigo propõe-se como objetivo principal propor e avaliar uma nova arquitetura das nuvens baseadas em IP MPLS em relação ao isolamento, separação dos planos de endereços e conectividade, com uma proposta de uma nova arquitetura hibrida baseada em IP MPLS.

A migração de um serviço baseado em uma arquitetura tradicional para uma arquitetura baseada em computação em nuvem significa transferir para o provedor de serviço da nuvem todo o controle e responsabilidade. Isso representa para o provedor de serviço um grande desafio, pois os riscos são os mais diversos possíveis, em função principalmente das diversas tecnologias que compõem o sistema em inter-cloud. A tabela I representa os principais riscos em computação em nuvem.

TABELA I
OS PRINCIPAIS RISCOS DA COMPUTAÇÃO EM NUVENS

Riscos	Definição
Interrupção de dados [3, 10, 12,14].	Os dados podem ser interceptados entre as nuvens ou entre os usuários e as nuvens, portanto uma nova arquitetura deve prover uma solução para esse problema
Disponibilidade [3,10,12]	A disponibilidade de um padrão de nuvens deve ficar no patamar de 99,99% para cima. A interrupção do serviço de nuvens pode representar a paralisação de vários negócios e grandes perdas financeiras
Interoperabilidade [3, 12,14]	A interoperabilidade entre nuvens deve permitir a comunicação de usuários em nuvens diferente como se estivessem em uma única nuvem global com qualidade de serviço e segurança
Isolamento [3,10,14]	Uma nova arquitetura deve evitar que usuários mal intencionados possam interromper os serviços de nuvens fornecidos pelos provedores, ou seja, deve existir um isolamento entre o plano de endereçamento do usuário e o plano de endereçamento do core da nuvem. Falhas de isolamento do usuário e a nuvem podem provocar acessos não autorizados a dados ou utilização indevida de recursos
Ataques DoS [3,12,14]	Uma nova arquitetura deve possuir mecanismo de proteção contra ataques de negação de serviço

III. MODELO PROPOSTO PARA A INTERCONEXÃO DAS NUVENS BASEADOS EM MPLS

As nuvens computacionais podem ser divididas basicamente da seguinte forma:

• Nuvens públicas: a infraestrutura da nuvem pertence a um provedor de serviço de nuvem computacional que vende os serviços entre diferentes usuários. Todos os usuários compartilham o conjunto de recursos providos pela infraestrutura que normalmente utiliza a internet como suporte para a comunicação, trazendo consigo todos os riscos de segurança e qualidade de serviço do protocolo IP público;

• Nuvens privadas: a infraestrutura da nuvem é projetada para uma organização, utilizando normalmente uma infraestrutura de rede fechada com maior nível de segurança e qualidade de serviço, podendo ser gerenciada pelo próprio usuário ou pelo provedor de serviço.

Diante desse cenário, o artigo propõe um modelo de computação em nuvem hibrida baseados nas tecnologias IP e MPLS. Esse novo modelo é baseado nas tecnologias IP e MPLS para oferecer segurança e qualidade de serviço nas conexões de duas ou mais nuvens, permitindo assim a portabilidade entre os dados e a interoperabilidade entre nuvens.

A. Separação/Isolamento de tráfego das Nuvens MPLS

A Fig. 2 apresenta a implementação de uma nuvem virtual utilizando MPLS. Essa nuvem é formada de quatro sites que se comunicam entre si. A nuvem virtual ABCD é formada por quatro sites da mesma organização que se comunicam através da conectividade IP MPLS. Os elementos da tecnologia MPLS e seu funcionamento básico são apresentados em [9].

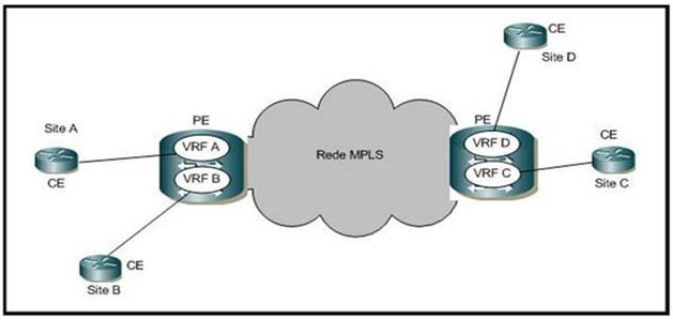

Figura 2. Nuvens MPLS.

Esse artigo propõe a implementação de nuvem virtual com a tecnologia MPLS que é realizada basicamente através dos parâmetros de RT (Route Target) e RD (Route Distinguishers).

Cada VRF (Virtual Routing Forward) no roteador de borda PE necessita ter um identificador de rotas associado, que pode estar relacionado a um site ou a uma nuvem. No caso mais comum, que é a formação de nuvem em que os usuários com interesse de conectividade que pertencem somente a uma nuvem. A nova proposta apresentada nesse artigo recomenda o uso de um único identificador de rotas RD que iremos chamar nesse artigo de identificador de nuvens para cada nuvem virtual. Para uma topologia de um modelo de nuvem virtual simples, como o da topologia apresentada na Fig. 1, a tabela 1 apresenta as configurações dos identificadores de nuvens RDs e RTs – usa-se o mesmo identificador de rotas por nuvem para reduzir o uso de memória do roteador de borda PE. O atributo RT [7] identifica uma coleção de VRFs pela qual um roteador PE distribui as rotas. Um roteador PE de uma nuvem aqui proposto utiliza esse atributo (RT) para restringir a importação e exportação de rotas para as VRFs. Cada VRF tem uma política de configuração para importação e exportação das rotas e o roteamento que é distribuído para outros PEs são marcados como atributos RT de exportação. As rotas que são recebidas pelo outro roteador PE são checadas para verificar se seu atributo RT de importação aceita inserir a rota na VRF. Esse mecanismo flexível permite a construção de diferentes topologias de nuvens e modelos de negócios. Esse atributo é definido em BGP Extended Communities Attribute [7,9,11]. Erros de configurações do RT cometidos pelo provedor de serviço de nuvens virtuais podem comprometer facilmente a segurança das nuvens MPLS virtuais, pois o RT é responsável por controlar quais rotas devem ser inseridas nas VRFs das nuvens. A combinação dos endereçamentos IP e os Identificadores de Rotas (RD) fazem com que as rotas sejam únicas através das nuvens virtuais MPLS. A tabela II apresenta um exemplo de configuração da nuvem virtual da Fig. 2. Nesse exemplo foi utilizado o mesmo RD para todos os sites da nuvem ABCD.

TABELA II
RD e RT das VRFs

Nuvem ABCD	RD	RT
VRF A	100	101
VRF B	100	101
VRF C	100	101
VRF D	100	101

Entretanto, se algum desses usuários no futuro pretender ser conectar entre nuvens para formar uma inter-cloud – por exemplo, suponha-se que um identificador de rotas é utilizado pela nuvem A, que esta tenha um usuário e que este precise ser membro de múltiplas nuvens, não será possível determinar que identificador de rotas virtuais (RD) usar porque ele pertence a mais de uma nuvem. Para tratar essa questão, quando certas topologias são criadas, pode ser necessário estender os identificadores de rotas virtuais por VRF/usuários para um determinado modelo de projeto, mas somente para projetos especiais, pois a criação de identificadores de rotas virtuais (RD) por site não oferece escalabilidade para o provedor de nuvem.

Para a proposta da arquitetura de nuvens virtuais baseada em MPLS se faz necessário: Definir as configurações dos roteadores virtuais que fazem parte da nuvem, Definir as configurações e identificador de rotas (RD) das nuvens, definir e configurar as politicas de importação e exportação de rotas das nuvens (RT), configurar os enlaces entre os roteadores dos usuários (CE/CPE) e os equipamentos de borda da nuvem MPLS (PE) e associar a interface do CE com os elementos PE do core das nuvens.

O primeiro passo no projeto de um serviço de nuvem, baseado na arquitetura MPLS, é definir e configurar o roteamento e encaminhamento virtual (VRF). No caso acima, isso significa configurar VRFs para a nuvem ABCD. Cada roteador PE deve ser conectado ao roteador CE do usuário que deseja receber rotas da nuvem específica. As configurações das VRFs virtuais devem existir em todos os roteadores PEs da nuvem.

IV. TESTE: CONECTIVIDADE E ISOLAMENTO DAS NUVENS IP MPLS

O objetivo é investigar a capacidade da nova proposta das nuvens baseadas em MPLS em conectar sites da mesma nuvem virtuais, isolar sites de diferentes nuvens, garantindo que o usuário não tenha acesso indevido aos equipamentos do núcleo da nuvem do provedor, e mostrar que, as nuvens baseadas em MPLS, os mesmos planos de endereços podem ser utilizados por diferentes usuários, desde que estejam em nuvens diferentes.

Para o teste, serão configuradas três nuvens: a nuvem azul, a nuvem verde e a nuvem vermelha, de acordo com a topologia apresentada na Fig. 3. A nuvem azul é formada pelos seguintes roteadores de acesso CEs: CE1, CE5, CE6 e CE9. A nuvem verde é formada pelos CEs: CE2, CE3 e CE7. A nuvem vermelha possui os CEs: CE4, CE8 e CE10. Os computadores C1 e C7 fazem parte das nuvens azul e verde respectivamente. O software utilizado para a avaliação de conectividade das nuvens será o comando ping, tratado brevemente a seguir.

A. *Material utilizado no teste para avaliar a nuvem MPLS*

Os materiais utilizados nos testes dividem-se em software e hardware. O software utilizado foi o comando ping, enquanto que o hardware foram roteadores, computadores, link de comunicações e uma infraestrutura de nuvem de um núcleo de rede que trabalha com o protocolo MPLS.

O comando ping está presente em grande parte dos sistemas operacionais e equipamentos de redes; nada mais é do que uma mensagem ICMP tipo echo request. O ICMP (Internet Control Message Protocol) apresenta como respostas que serão úteis na análise de conectividade das nuvens MPLS as seguintes mensagens de respostas:

(i) Destination host unreachable
Host Unreachable (Host Inalcançável) – Mensagem recebida de um roteador.
Causa: a rede destino foi alcançada, mas não foi possível entregar o pacote para o host destino, provavelmente por causa de uma submáscara configurada erroneamente ou porque o host destino não está acessível.

(ii) Request timed out
O pacote foi enviado com sucesso ao destino, mas a resposta foi bloqueada ou perdida. Outra possibilidade para essa mensagem é que a resposta poderá ser bloqueada ou descartada em algum roteador que fica no caminho de retorno.

B. *Topologia para o teste de avaliação da proposta*

A topologia apresentada na Fig. 3 representa o ambiente para o teste e avaliação da arquitetura proposta baseada em MPLS.

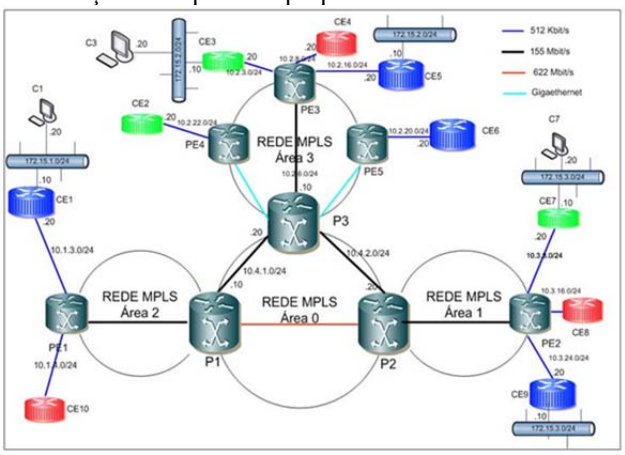

Figura 3. Ambiente de teste para a arquitetura em nuvem MPLS.

C. *Testes Realizados da Nova Proposta de nuvem*

Do computador C1 da nuvem Azul, que foi configurada para essa nuvem, tentar conectar-se, através do comando ***ping***, aos roteadores CE1, CE5, CE6 e CE9, que pertencem à mesma nuvem Azul, esse teste avaliará a capacidade de interconexão das nuvens MPLS. O segundo teste será do C1 da nuvem Azul, que foi configurada, tentar conectar-se ao C7 da rede 172.15.3.0/24, que possui o mesmo endereço da rede 172.15.3.0/24 do CE9, mas está em nuvem diferente (RD: Identificadores das nuvens virtuais são diferentes), ou seja, na nuvem verde [11], esse teste avalia a capacidade da nova proposta em conectar sites com o mesmo endereço em nuvens diferentes. A próxima análise será do C1 da nuvem azul, tentar conectar-se, através do comando ***ping***, aos roteadores CE2, CE3, CE7 e ao Computador C7, que pertencem à nuvem verde, esse teste avalia a capacidade de isolamento das nuvens MPLS quando configuradas devidamente pelos provedores de nuvens. Do C7 da nuvem verde, tentar conectar-se ao roteador CE1 da nuvem azul. Do C7 da nuvem verde, tentar conectar-se ao roteador CE3 e ao C3 da nuvem verde, esse teste avalia a

capacidade de conectividade entre os sites da nuvem verde. O C1 da nuvem azul, tentar conectar-se ao P1, P2 e P3, esse teste avaliou a segurança do core (P1, P2 e P3) do provedor quando um usuário tenta atacar o provedor de nuvem.

V. RESULTADOS DOS TESTES

Os resultados dos testes realizados para posterior avaliação foram coletados conforme comando do item IV e são apresentados de forma resumida nas tabelas abaixo neste tópico. Todos os resultados dos testes não foram apresentados de forma detalhada em função do limite de páginas possíveis do artigo.

A. Do computador C1que está na nuvem Azul, testar a conectividade com CE1, CE5, CE6 e CE9

O computador C1 tenta conectar-se com o roteador CE1(10.1.3.20)

```
d:\>ping 10.1.3.20
Pinging 10.1.3.20 with 32 bytes of data:
Reply from 10.1.3.20: bytes=32 time<10ms TTL=255
Reply from 10.1.3.20: bytes=32 time<10ms TTL=255
Reply from 10.1.3.20: bytes=32 time<10ms TTL=255
Reply from 10.1.3.20: bytes=32 time<10ms TTL=255
Ping statistics for 10.1.3.20:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

TABELA III
C1 TENTA SE CONECTAR A CE1, CE5, CE6 E CE9

	CE1	CE5	CE6	CE9
C1	**CONECTOU COM ÊXITO** Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)	**CONECTOU COM ÊXITO** Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)	**CONECTOU COM ÊXITO** Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)	**CONECTOU COM ÊXITO** Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

B. O computador C1 tentará conectar-se ao computador C7

TABELA IV
C1 TENTA SE CONECTAR AO C7

	C7
C1	Request timed out. **NÃO CONECTOU** Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C. Computador C1 tentará conectar-se aos roteadores CE2, CE3, CE7 e ao computador C7.

TABELA V
C1 TENTA SE CONECTAR A CE2, CE3, CE7 E C7

	CE2	CE3	CE7	C7
C1	**NÃO CONECTOU.** Reply from 172.15.1.10: Destination host unreachable	**NÃO CONECTOU.** Reply from 172.15.1.10: Destination host unreachable	**NÃO CONECTOU.** Reply from 172.15.1.10: Destination host unreachable	**NÃO CONECTOU.** Request timed out.

D. O computador C7 tentará conectar-se ao roteador CE1 da nuvem Azul.

TABELA VI
C7 TENTA SE CONECTAR AO CE1

	CE1
C7	Não conectou. Reply from 172.15.3.10: Destination host unreachable

E. O computador C7 tentará conectar-se ao roteador CE3 e ao computador C3 da nuvem Verde

TABELA VII
C1 TENTA SE CONECTAR A CE2, CE3, CE7 E C7

	CE3	C3
C7	Conectou. Packets: Sent = 4, Received = 4, Lost = 0	Conectou. Packets: Sent = 4, Received = 4, Lost = 0

F. Do computador C1, tentar conectividade com os roteadores de núcleo da nuvem P1, P2 e P3.

TABELA VIII
C7 TENTA SE CONECTAR AO CORE DA NUVEM

	P1	P2	P3
C7	Não conectou. Reply from 172.15.1.10: Destination host unreachable	Não conectou. Reply from 172.15.1.10: Destination host unreachable	Não conectou. Reply from 172.15.1.10: Destination host unreachable

VI. ANÁLISE DE RESULTADOS

O primeiro resultado dos testes mostrou a capacidade de conectividade entre os elementos que pertencem à nuvem azul. O computador C1 faz tentativa e obtém total sucesso ao conectar-se ao roteador CE1. O mesmo resultado foi alcançado para as tentativas do C1 quando este tentou conectar-se aos roteadores CE5, CE6 e CE9; todos os pacotes transmitidos foram recebidos. O segundo resultado dos testes do item refere-se à capacidade das nuvens MPLS para trabalhar com os mesmos endereços IPs, desde que estes sejam de nuvens diferentes. O endereço IP do C7 é 172.15.3.20, que é o mesmo endereço do roteador CE9, mas pertencente à nuvem verde. Ao tentar conectar-se ao CE7 através do comando PING, a resposta ao comando foi uma negação às tentativas de conexão. Esse resultado confirmou a capacidade das nuvens MPLS de vários usuários do provedor em utilizar os mesmos endereços IP, desde que sejam utilizados em nuvens diferentes. O terceiro resultado dos testes de avaliação mostrou a capacidade das nuvens MPLS em isolar o tráfego entre as nuvens. O computador C1, que pertence à nuvem azul, tentou conectar-se aos roteadores CE2, CE3, CE7 da nuvem verde e ao computador C7 que também pertence a nuvem verde. Nenhuma das quatro tentativas de conectar-se à nuvem verde obteve sucesso. O quarto resultado dos testes da avaliação mostra a capacidade de isolamento entre as nuvens verde e azul. O computador C7 da nuvem verde tenta conectar-se com o roteador CE1 da nuvem azul e não obtém sucesso, pois estão em nuvens diferentes. O quinto teste avalia a conectividade entre os sites da nuvem verde; para isso, o computador C7 da nuvem verde tenta conectar-se ao roteador CE3 e ao computador C3. Os resultados mostram que o computador C7 obteve total sucesso em suas solicitações de conexões para o CE3 e o C3. O último teste avaliou o nível de segurança das nuvens MPLS quando um usuário mal-intencionado tenta invadir os roteadores P1, P2 e PE3 do núcleo das nuvens MPLS. Nenhuma das três tentativas obteve sucesso. Isso mostra que a única forma de um usuário acessar o núcleo de

uma nuvem MPLS é se o provedor implementar alguma configuração específica que possa permitir o acesso ou cometa alguma falha de configuração no core da nuvem MPLS.

VII. CONCLUSÃO

Este artigo avaliou a capacidade de uma proposta de nuvens baseadas em IP MPLS de oferecer isolamento e conectividade para as nuvens computacionais dos provedores de serviços de nuvens. Os resultados mostraram que as propostas baseadas em nuvens IP MPLS são totalmente seguras, desde que configuradas devidamente pelo provedor de serviço de nuvens. Os testes avaliaram a conectividade entre as três nuvens (Azul, Verde e Vermelha) quando elas utilizam o mesmo plano de endereçamento IP, pois um dos pontos fundamentais das novas arquiteturas de nuvens baseadas em IP MPLS é que seja possível conectividade entre nuvens que utilizam os mesmos endereços, permitindo uma otimização dos endereços IP disponíveis. Os resultados do teste mostram que existe conectividade entre os CEs da mesma nuvem, mesmo que existam outros endereços iguais, mas em outra nuvem. Os testes também avaliaram a capacidade de isolamento entre as três nuvens. Nesse teste de MPLS, foi mostrada a sua capacidade de separação de endereçamento e roteamento. As tabelas abaixo apresentam um resumo das conexões e as não conexões que foram possíveis.

TABELA IX
RESULTADOS DOS TESTES

	CE1	CE2	CE3	CE5	CE6	CE7
C1	OK	X	X	OK	OK	X
C7	X	-	OK	-	-	-

OK=CONECTOU COM EXITO
X = NÃO CONECTOU

TABELA X
RESULTADOS DOS TESTES

	CE9	C3	C7	P1	P2	P3
C1	OK	-	X	X	X	X
C7	-	OK	-	-	-	-

OK=CONECTOU COM EXITO
X = NÃO CONECTOU

REFERÊNCIAS

[1] Arun Katara, Rajkumar Chalse, Ashwin Selokar: A New Technique of Data Integrity for Analysis of the Cloud Computing Security 2013 5th International Conference on Computational Intelligence and Communication Networks, IEEE computer society.

[2] Christina N. Hoefer and Georgios Karagiannis: Taxonomy of cloud computing services. In Proceedings of the 4th IEEE Workshop on Enabling the Future Service- Oriented Internet, EFSOI'10, pages 1345–1350, December 2010.

[3] ENISA. Cloud computing: Benefits, risks and recommendations for information security. Technical report, European Network and Information Security Agency (ENISA), November 2009. Disponível emhttp://www.enisa.europa.eu/activities/riskmanagement/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. Acessado em 09 de julho de 2013.

[4] Jingxin K. Wang, Jianrui Ding, and Tian Niu. Interoperability and Standardization of Intercloud Cloud Computing, Dec 2012.

[5] Markus Endler, José Viterbo e Hubert Fonseca, Perspectivas e Desafios da Computação em Nuvem na Internet do Futuro, Relatório PUC-RJ, 2011

[6] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, and Matei Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical report, Electrical Engineering and Computer Sciences University of California at Berkeley, 2009.

[7] Michael H. Behringer, Monique J. Morrow. "MPLS VPN Security", Cisco Press 2005

[8] Michael Kretzschmar and Mario Golling; Security Management Spectrum in future Multi-Provider Inter-Cloud Environments Method to highlight necessary further development; IEEE 2011

[9] Monique Morrow, Azhar Sayeed. "MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization", 2006.

[10] Ronald L. Krutz and Russell Dean Vines. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. John Wiley & Sons, Inc., August 2010.

[11] RFC - Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs) http://www.faqs.org/rfcs/rfc4381.html, Acesso em 25/06/2012.

[12] Shashikala P. Subashini and Veeraruna R. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1 – 11, 2011.

[13] Soares Anderson, Ferreira, "Uma arquitetura para monitoramento de segurança baseada em acordos de níveis de serviço para nuvens de infraestrutura", Dissertação de Mestrado, Unicamp, 2013

[14] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Series. O'Reilly Media, 2009.

[15] Yanpei Chen, Vern Paxson, and Randy H. Katz. What's new about cloud computing security? Technical Report UCB/EECS-2010-5, Electrical Engineering and Computer Sciences University of California at Berkeley, January 2010.

Adao Boava, received his B.S. degree in Electrical Engineering in 1991 from Federal University of Santa Catarina (UFSC), Florianopolis-SC, Brazil. He received his M.S. degree from the State University of Campinas (Unicamp), and M.B.A. from Foundation Getulio Vargas (FGV), São Paulo, Brazil. In 2011, he received his PhD in Telecommunication Engineering and Telematics from Unicamp, São Paulo, Brazil. Currently, he is a professor at Federal University of Santa Catarina (UFSC), Santa Catarina, Brazil. He has worked in Brasil Telecom and OI for 16 years with MPLS product development. In addition, he has worked as a consultant in different data communication projects for Monsanto, Santander, Itau, Visa, Redecard and others.

Yuzo Iano, received his PhD. in electrical engineering in 1986. Currently he is an Associate Professor in Electrical Engineering at Unicamp (State University of Campinas, Brazil). He also works at the Visual Communication Laboratory in the same University and is responsible for digital signal processing (sound and image) projects. His research interests include video and audio coding, digital video and audio compression and digital signal transmission. He is a member of IEEE.