Validação do ESG Labs

Cisco Application Centric Infrastructure (ACI)

Rede definida por software escalável, automatizada, segura e aberta para impulsionar a transformação digital

Por Tony Palmer e Kerry Dolan, analistas seniores de validação de TI

Outubro de 2017

Este relatório comparativo produzido pelo ESG Labs foi autorizado pela Cisco Systems e é distribuído mediante licença do ESG.

Conteúdo

Relatórios laboratoriais do ESG

O objetivo dos relatórios laboratoriais do ESG é instruir profissionais de TI em relação a produtos de tecnologia de informação para empresas de todos os tipos e tamanhos. Os relatórios do ESG não substituem o processo de avaliação que deve ser realizado antes de tomar decisões de compra, apenas fornecem informações sobre essas novas tecnologias. Nosso objetivo é rever algumas das funções/recursos mais valiosos dos produtos, mostrar como eles podem ser usados para resolver problemas reais do cliente e identificar áreas que necessitam de melhoria. A perspectiva dos especialistas terceirizados do ESG Labs tem como base nossos testes práticos, bem como entrevistas com os clientes que utilizam estes produtos em ambientes de produção.

Introdução

O ESG conduziu testes práticos e completos da ACI (Infraestrutura Centrada em Aplicações) da Cisco com foco em desempenho, disponibilidade, segurança e simplicidade operacional, realizando os mesmos testes em comparação com uma solução de rede definida somente por software (SDN).

Resumo executivo

As empresas hoje em dia enfrentam desafios para acompanhar as demandas de clientes em constante mudança e sempre se deparam com ameaças competitivas. Para terem sucesso, as empresas precisam ser muito mais ágeis e focadas em fornecer uma experiência superior ao cliente. Isso exigirá adaptações e, em muitos casos, atualização de processos, cultura e tecnologia; comumente chamada de transformação digital. Será essencial garantir que todos os aplicativos sejam implantados rapidamente, tenham desempenho ideal, permaneçam altamente disponíveis e sejam seguros. Para fazer essa transformação, as empresas precisam implantar tecnologias que utilizem os recursos definidos por software, mas que também permaneçam simples de operar e automatizar. A Cisco projetou a ACI para ser um facilitador-chave da transformação digital.

Validação pelo Laboratório do ESG

No teste de VM para servidor bare metal, o laboratório do ESG descobriu que a Cisco ACI forneceu latência até 80% menor, taxa de transferência até 600% maior e uma melhoria de até 40% nas transferências de arquivos grandes entre uma VM e um servidor bare metal.

No geral, o laboratório do ESG concluiu que o desempenho da Cisco ACI é coerente e previsível em todos os testes. Em cenários realistas, em que o tráfego que flui pelo ambiente é dinâmico e muitas vezes imprevisível, envolvendo aplicativos e sistemas virtualizados ou não, a ACI fornece consistentemente a menor latência e melhor produtividade, com o desempenho previsível exigido por aplicativos de missão crítica.

A Cisco ACI utiliza uma arquitetura ativa-ativa para alta disponibilidade em todos os caminhos de rede, com convergência inferior a um segundo em condições de falha. O laboratório do ESG observou que, na solução concorrente, a disponibilidade ativa-ativa estava limitada ao uso de ECMP (roteamento de múltiplos caminhos) com mesmo custo, que funciona para roteamento, mas não para outros serviços de rede críticos, como segurança e NAT. Esquemas de disponibilidade em espera ativa são abaixo do ideal para aplicativos modernos essenciais para a missão e os negócios. Examinando os elementos de trabalho das duas soluções testadas, o laboratório do ESG observou que a ACI tem 50% menos vetores de falha em comparação com a solução competitiva. O teste de laboratório do ESG também confirmou o impacto zero ou os tempos de convergência de failover inferiores a um segundo em todos os testes de disponibilidade. Na opinião do laboratório do ESG, a ACI é uma excelente escolha para aplicativos essenciais à missão e aos negócios.

As violações do data center geralmente ocorrem dentro do próprio data center. Com o modelo de segurança de lista de permissão, a ACI fornece uma solução de microssegmentação onipresente. A aplicação de regras e políticas de segurança no nível da rede é complicada, pois os profissionais de TI precisam garantir que todos os elementos na rede do data center apliquem regras e políticas consistentemente para todos os tipos de tráfego de rede. O laboratório do ESG testou a capacidade da Cisco ACI de fornecer suporte de microssegmentação compatível com as cargas de trabalho em vários hypervisors, endpoints bare metal e contêineres, em data centers conectados por meio de uma WAN. A Cisco ACI forneceu uma imposição de segurança granular do endpoint em ambos os data centers, com políticas definidas usando objetos do VMware vCenter. Realizamos o mesmo teste com a solução SDN somente de software e descobrimos que, quando tentamos aplicar as mesmas diretivas de firewall às mesmas cargas de trabalho nos data centers com diferentes servidores vCenter, essas diretivas não são aplicadas.

O ESG ficou particularmente impressionado com a facilidade de implantar aplicativos de multicamada usando os playbooks Ansible fornecidos pela Cisco ACI. Além disso, o modelo de virtualização de rede de sobreposição integrada permite que a ACI forneça automação muito mais rapidamente do que a solução SDN somente de software testada pelo ESG, ao mesmo tempo em que consome menos recursos. O laboratório do ESG automatizou o provisionamento de um ambiente de nuvem privada usando o Ansible com a ACI mais de 40 vezes mais rápido do que seria possível com o SDN somente de software. O laboratório do ESG também confirmou uma economia significativa na capacidade de computação e armazenamento, pois a ACI não exige VMs adicionais para executar serviços de roteamento e gateway.

A tecnologia Cisco ACI funcionou perfeitamente, independentemente da virtualização ou das tecnologias de empacotamento de aplicativos utilizadas. Os ambientes do cliente geralmente são uma mistura de vários hypervisors, e a configuração do teste de ACI poderia ter incluído facilmente os Hyper-V, KVM e Kubernetes/contêineres e obtido os mesmos resultados operacionais e funcionais, até mesmo entre VMs em diferentes hypervisors. No entanto, para garantir a imparcialidade da comparação com a solução SDN somente de software, que não sustenta tal funcionalidade, esses testes foram excluídos.

O ESG descobriu que a Cisco ACI fornece uma rede simples, escalonável e altamente disponível que é adequada às cargas de trabalho de missão crítica. Se a empresa estiver interessada em melhorar a automação, a agilidade, a segurança e a disponibilidade das redes em vários data centers híbridos, o laboratório do ESG recomenda uma análise mais detalhada da Cisco ACI.

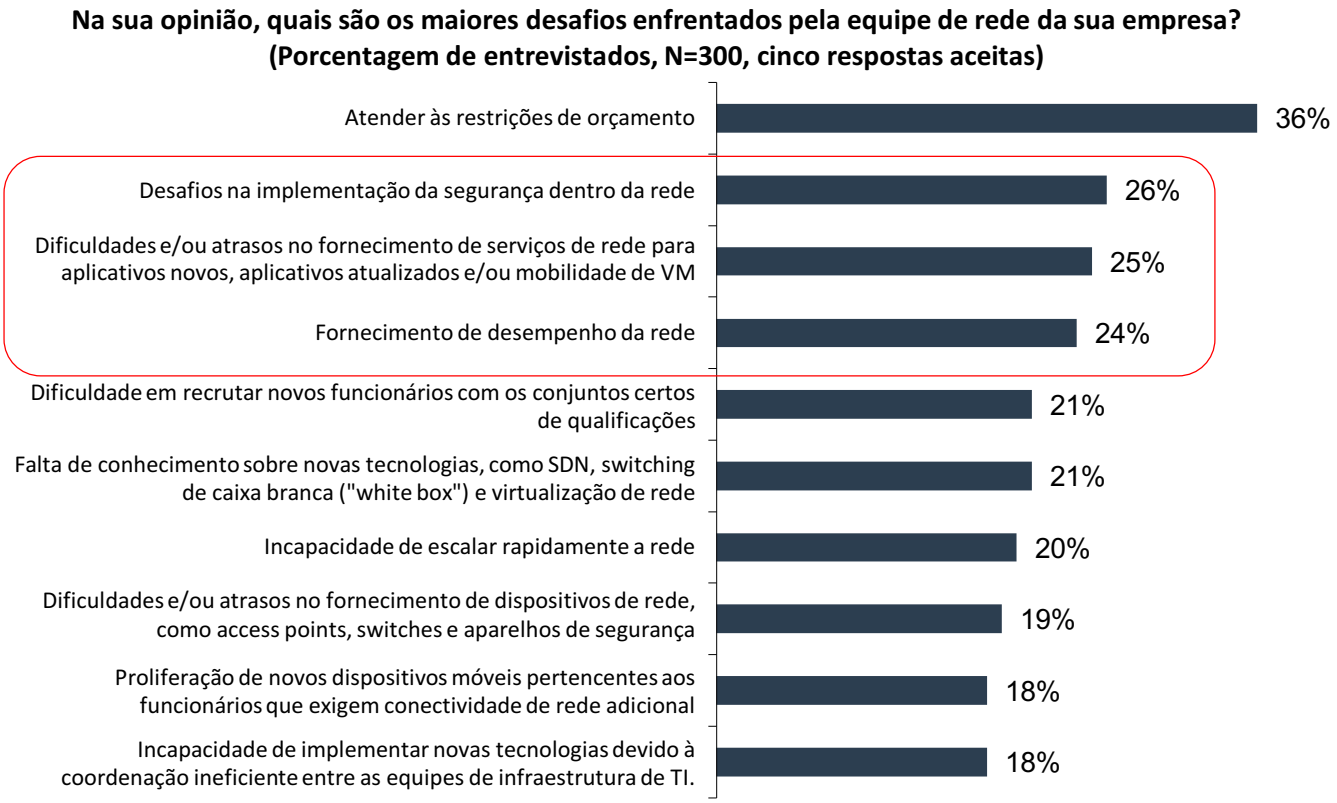
O que aparecerá em segundo plano

Uma rede ágil e consistentemente de alto desempenho é essencial para a computação de data center. Cada parte do negócio — e, algumas pessoas argumentam, quase tudo o que acontece na vida hoje — é afetada pela saúde e funcionalidade da rede, à medida que os funcionários acessam dados e aplicativos de vários locais, em diversos dispositivos. No entanto, à medida que as redes se expandem para lidar com os negócios de escala da Web atuais, elas se tornam mais complexas e difíceis de gerenciar, gerando problemas de desempenho e tempo de atividade e frustrando os usuários. Além disso, uma ameaça constante de invasão de rede pode resultar em danos irreparáveis, incluindo perda de dados, falha de conformidade e danos à reputação, mantendo a segurança de rede em primeiro plano para os profissionais de TI.

Uma pesquisa recente do ESG destaca essas realidades. Quando questionados sobre os maiores desafios de rede, os participantes da pesquisa de ESG citaram a implementação de segurança de rede, o provisionamento de serviços de rede para aplicativos e máquinas virtuais móveis (VMs) e o desempenho entre os principais desafios, colocando-os logo atrás das restrições orçamentárias (consulte a Figura 1).[1]

[1] Fonte: Pesquisa do ESG, *Network Modernization Trends*, julho de 2017.

Figura 1. Dez principais desafios de rede



Fonte: Enterprise Strategy Group, 2017.

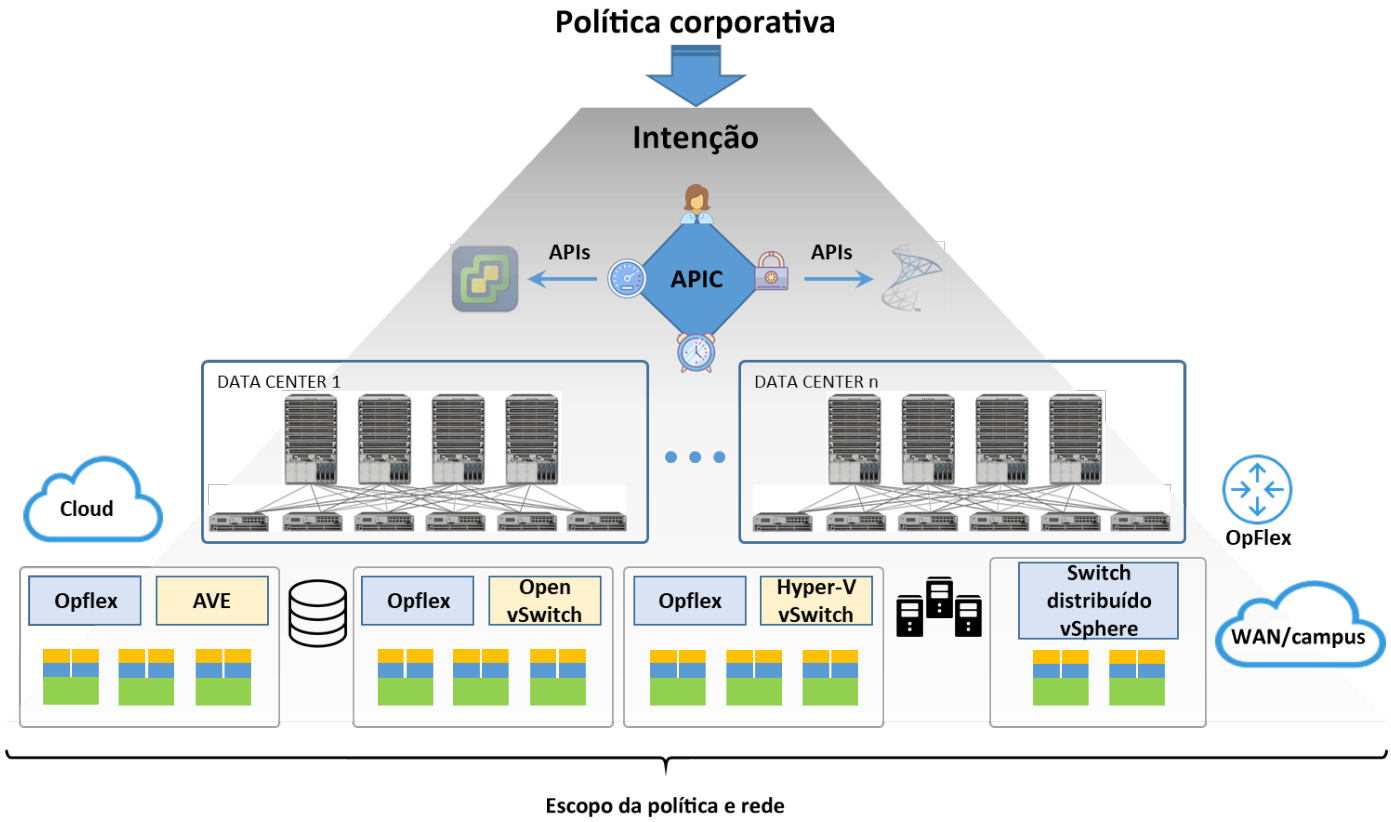
A rede definida por software pode simplificar o controle e as operações de rede ao abstrair os planos de controle e dados do hardware subjacente. Com a criação de componentes de rede lógicos, programáveis e dinâmicos baseados em componentes físicos de alta qualidade, a SDN pode oferecer serviços de rede mais confiáveis, rápidos e fáceis de projetar, gerenciar e solucionar problemas.

Cisco ACI

A Cisco ACI é uma solução de rede definida por software que combina elementos físicos e virtuais com o objetivo de simplificar operações de rede e o gerenciamento e oferecer serviços de rede centrados em aplicativos. A Cisco ACI foi projetada para escalar 400 switches e 180.000 endpoints. Com o modelo de sobreposição integrado da ACI, os clientes podem automatizar tarefas de rede comuns para simplificar o trabalho, além de permitir que eles evoluam para serviços de rede baseados em aplicativos e controlados por políticas. Com uma plataforma comum para ambientes físicos, virtuais e em nuvem, a Cisco ACI fornece visibilidade e controle centralizados para que os administradores possam gerenciar e solucionar problemas de serviços de rede em todo o ambiente. A ACI oferece microssegmentação para qualquer carga de trabalho. Em ambientes virtualizados, a microssegmentação da ACI é dimensionada de forma transparente entre os hypervisors e os data centers com base nos atributos da VM; além disso, simplifica o processo de implantação e dimensionamento da rede e melhora a segurança. A arquitetura da Cisco ACI apresenta menos vetores de falha do que as soluções SDN somente de software, permitindo que ele falhe com menos frequência e se recupere mais rapidamente de falhas de rede comuns (ou seja, falhas de nó de rede ou de link). Além disso, a Cisco ACI fornece visibilidade de hardware para entender os fluxos de tráfego, de modo que os administradores possam compreender melhor as falhas e corrigi-las.

Como visto na Figura 2, o Cisco Application Policy Infrastructure Controller (APIC) se integra às camadas de comutação física e virtual, incluindo opções de código aberto e de terceiros, para criar a base para um modelo de política que adapta serviços de rede e segurança a aplicativos e garante o alinhamento com as políticas de negócios.

Figura 2. Infraestrutura Centrada em Aplicativos da Cisco



Fonte: Enterprise Strategy Group, 2017.

Application Policy Infrastructure Controller (APIC)

O Cisco APIC[2] oferece acesso centralizado e controle a todas as informações de estrutura e switches virtuais gerenciados, com o objetivo de otimizar o ciclo de vida do aplicativo para melhor desempenho e escalabilidade. Para este fim, o APIC comporta rede flexível e provisionamento de políticas em recursos físicos e virtuais. Ele consiste em um cluster de controlador de, no mínimo, três nós que gerencia e opera a estrutura de ACI e os switches virtuais conectados. O cluster do APIC permite a sincronização e o gerenciamento do estado da rede de endpoint em vários gerenciamentos de máquina virtual (VMM) e domínios físicos. O software de estrutura da Cisco ACI fornece um sistema operacional de switch baseado em objeto, programável por meio de uma API REST aberta, que pode gerenciar os componentes subjacentes usando o protocolo OpFlex; isso cria uma estrutura aberta que permite a automação de rede voltada para aplicativos e de políticas.

Switches Cisco Nexus 9000 Series

O Nexus 9000 Series[3] é projetado para fornecer alto desempenho, alta densidade, baixa latência e economia de energia em uma variedade de fatores de forma com configurações Ethernet de 1/10/25/40/50/100 G. Os switches podem operar

[2] Para saber mais sobre o APIC, acesse: https://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html

[3] Para saber mais sobre o Nexus 9000 Series, acesse: https://www.cisco.com/c/pt_br/products/switches/nexus-9000-series-switches/index.html#~stickynav=1?CCID=cc000088

no software Cisco NX-OS ou nos modos de Infraestrutura Centrada em Aplicações (ACI) usando a tecnologia ASIC com escala de nuvem da Cisco. Eles são apropriados para implantações de data center tradicionais ou totalmente automatizadas.

Cisco Application Virtual Switch (AVS)/Application Virtual Edge (AVE)

O Cisco AVS e o AVE, a próxima geração do AVS, são componentes de software de estrutura da Cisco ACI. Eles compreendem um switch virtual distribuído e desenvolvido especificamente, integrado à plataforma de gerenciamento e orquestração da ACI, para automatizar o provisionamento de rede virtual. O AVS/AVE foi projetado para oferecer diferentes opções de encaminhamento e encapsulamento, direcionamento de tráfego para serviços de aplicativos e inspeção stateful em muitos hosts e data centers virtualizados do VMware vCenter. O AVS e o AVE da Cisco são integrados à arquitetura da Cisco ACI como um leaf virtual e são gerenciados pelo Cisco APIC. O Cisco AVS implementa o protocolo OpFlex para comunicação do plano de controle com o APIC.

A Cisco anunciou recentemente que a Cisco ACI estará disponível em ambientes de nuvem pública. A nova oferta, chamada Cisco ACI Anywhere, alavancará o Cisco AVE, a próxima geração do Cisco AVS. A premissa de Cisco ACI Anywhere é fornecer aos clientes da Cisco a flexibilidade de executar aplicativos em suas próprias nuvens privadas, bem como nas nuvens públicas de sua escolha, enquanto mantêm políticas de rede confiáveis em todo o domínio em várias nuvens.

Switching virtual OpFlex e de terceiros

A Cisco ACI usa um modelo de controle declarativo baseado no controle escalonável de objetos inteligentes. O controle declarativo determina que cada objeto seja solicitado a atingir um estado desejado e faz uma promessa de atingir esse estado, sem precisar informar exatamente como fazê-lo. Ele difere do modelo imperativo mais tradicional, que deve especificar cada elemento da configuração de baixo nível para atingir o estado desejado. A Cisco ACI utiliza o controle declarativo para separar os requisitos de aplicativo, operação e infraestrutura e permite que cada um seja especificado independentemente. O protocolo OpFlex é o mecanismo usado pela Cisco ACI para implementar o controle declarativo, a fim de transferir a política abstrata de um controlador de política de rede para um conjunto de dispositivos smart capazes de renderizar a política abstrata.

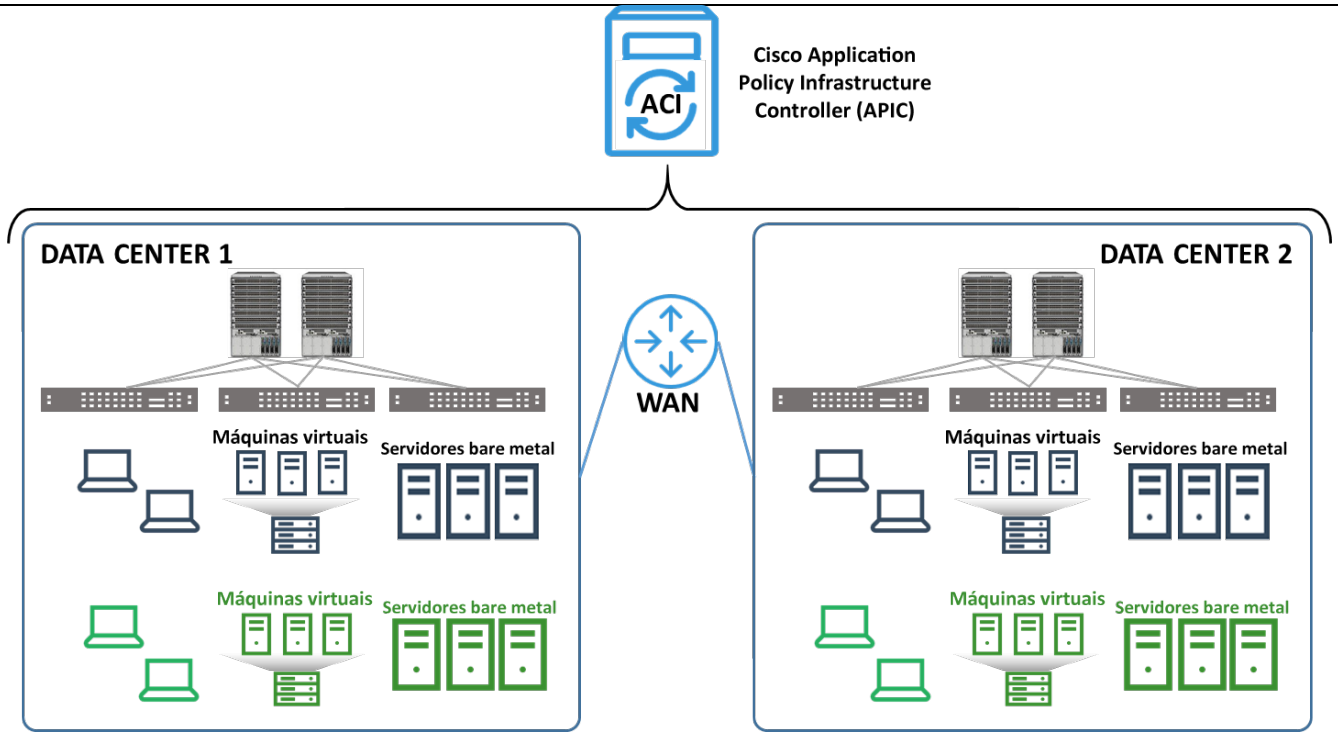
Além do AVS e do AVE da Cisco, a Cisco ACI usa o protocolo OpFlex para funcionar com o Open vSwitch (OVS) e o switch virtual Microsoft Hyper-V. O APIC também aproveita as APIs em direção ao norte para interagir com outros vSwitches de terceiros, como o VMware VDS. O OpFlex também é usado para interagir com determinados roteadores e switches da Cisco, como o Nexus 7000, o ASR 1000 e o ASR 9000.

Validação do laboratório ESG

O laboratório do ESG realizou avaliações e testes práticos da Cisco ACI e comparou os resultados com uma solução SDN somente de software. O teste foi desenvolvido para demonstrar o desempenho, a disponibilidade, a segurança e a automação fornecidos pela ACI em um ambiente empresarial moderno e distribuído com servidores físicos e virtuais que abrangem vários data centers.

A bancada de teste foi projetada para simular um ambiente de cliente com vários data centers e uma mistura de servidores virtualizados e bare metal que comportam ambientes de produção e desenvolvimento (veja Figura 3). Os ambientes do cliente geralmente hospedam uma mistura de vários hypervisors, e a configuração do teste de ACI poderia ter incluído facilmente o VMware, Hyper-V, KVM e Kubernetes/contêineres para demonstrar os mesmos resultados operacionais e funcionais, até mesmo entre VMs em diferentes hypervisors. No entanto, para garantir uma comparação imparcial com outra solução SDN, que não comporta tal funcionalidade, esses testes foram excluídos.

Figura 3. A plataforma de teste do ESG Lab



Fonte: Enterprise Strategy Group, 2017.

Desempenho

O laboratório do ESG testou o desempenho da Cisco ACI em comparação a uma solução somente de software em vários cenários projetados para simular casos de uso comuns implantados por empresas no mundo real: carga de trabalho em execução entre máquinas virtuais hospedadas em um hypervisor em um único host, entre máquinas virtuais em hosts diferentes e entre máquinas virtuais e servidores bare metal.

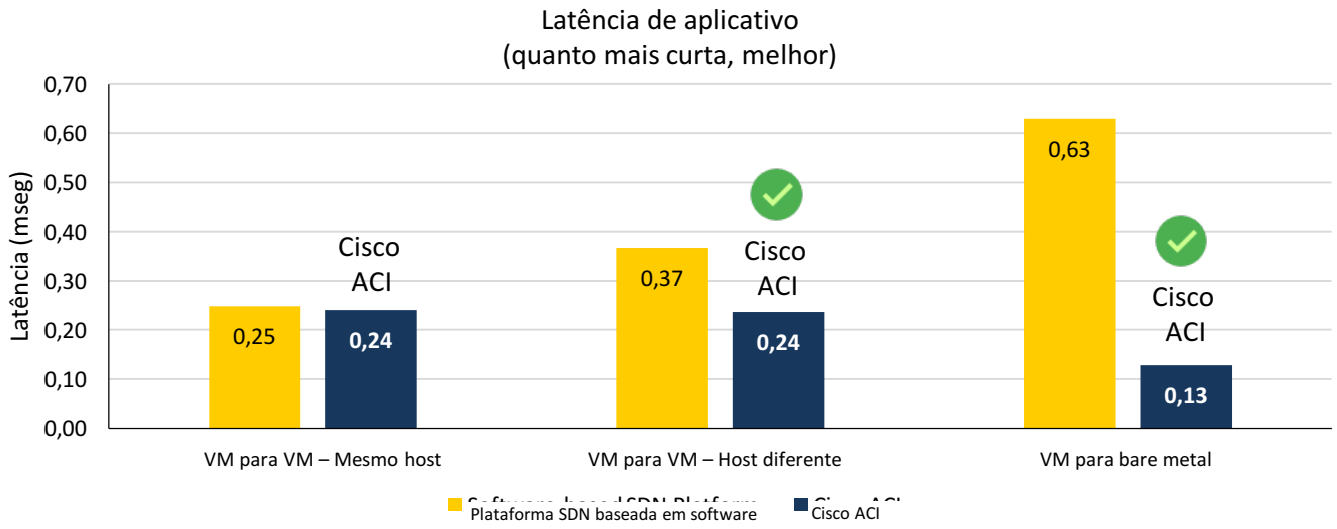
Teste do ESG Lab

O teste de desempenho é amplamente dependente de aplicativos e muitos fatores contribuem para a compreensão dos resultados. A infraestrutura de rede, a produtividade e a latência de armazenamento, o software de aplicativo e o planejador de hypervisor são todos fatores que podem afetar o desempenho de alguma forma. O laboratório do ESG selecionou três métricas simples para medir o desempenho da Cisco ACI em comparação com uma plataforma SDN somente de software.

A latência do aplicativo foi medida usando o Linux nmap versão 6.40. A produtividade de rede foi testada usando o Linux iPerf3 com tamanhos de segmento máximo (MSS) de 250, 500 e 1.448 bytes. A produtividade do aplicativo foi testado com o download de um arquivo de 7 GB usando dois protocolos diferentes: uma transferência de arquivo HTTP usando o *wget* do Apache em execução no CentOS. Todos os testes usaram servidores Cisco C220-M4L com dois Xeon E5-2650, CPUs de 10 núcleos. O LRO (Large Receive Offload) e o TSO (TCP Segmentation Offload) foram ativados nos níveis de host e convidado, e o RSS (Receive Side Scaling) foi ativado em todos os hosts com NICs compatíveis com VXLAN. Todas as VMs usadas para teste foram criadas em um único modelo com configurações idênticas de vCPU, memória e rede. Como os resultados dos testes em plataformas x86 virtualizadas podem variar ligeiramente entre as iterações individuais, cada teste foi executado dez vezes e a média dos resultados foi calculada para torná-los mais precisos e confiáveis.

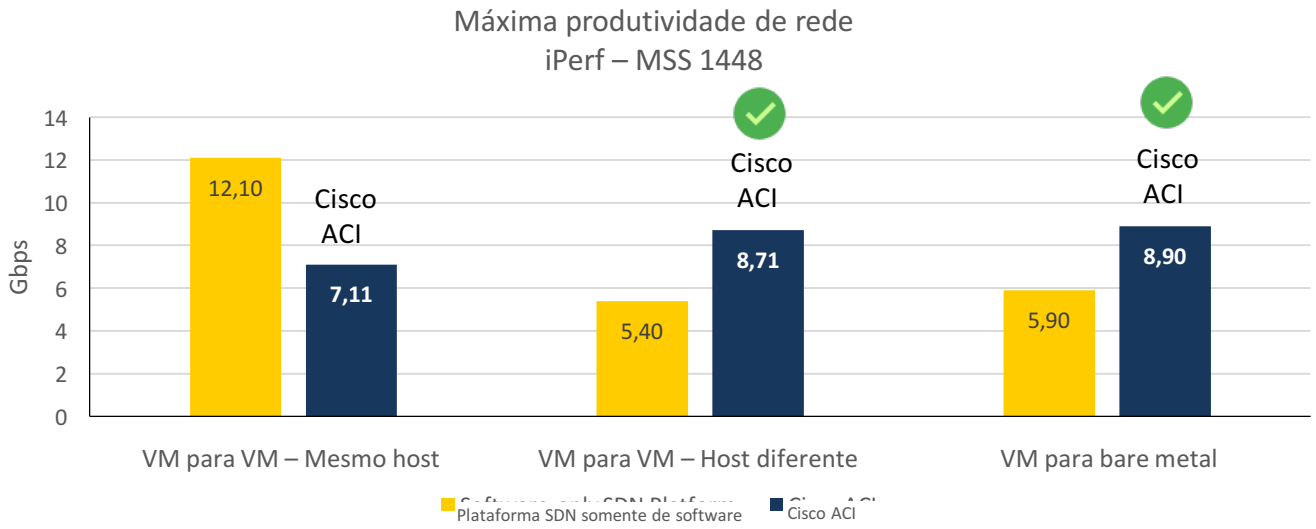
Figura 4 mostra a latência entre VMs no mesmo hypervisor, em hypervisors diferentes e de uma VM para um bare metal. Em todos os casos, a Cisco ACI mostrou uma vantagem, com a ACI fornecendo uma latência 80% menor do que a solução SDN somente de software em execução em máquinas virtuais.

Figura 4. Latência de aplicativo



Em seguida, a produtividade de rede foi testada usando iPerf3. Nesses testes, a plataforma SDN somente de software proporcionou melhor desempenho quando as duas VMs estavam no mesmo host, mas quando o tráfego precisou ser cruzado para um host diferente ou usando um servidor bare metal não virtualizado, a Cisco ACI demonstrou vantagens. Figura 5 mostra os resultados com MSS definido como 1.448, onde a vantagem de desempenho da ACI foi 61% em VM para tráfego de servidor bare metal. Em testes com tamanhos de segmento menores, a diferença foi mais evidente. Em um MSS de 500 bytes, a produtividade da ACI para a mesma VM de teste de bare metal foi 3,8 vezes maior que a do SDN somente de software. Com um MSS de 250, a produtividade da ACI entre VMs e servidores bare metal foi 6 vezes maior que a solução de somente de software.

Figura 5. Produtividade de rede usando iPerf3



É importante observar que, nos testes de VM para VM no mesmo host, o uplink de rede de 10 Gbps foi um gargalo para a ACI, pois o tráfego entre as VMs flui pelo switch leaf. A Cisco sustenta que um uplink de 25 Gbps teria permitido que a ACI atingisse uma produtividade comparável.

Por fim, analisamos as transferências de um arquivo de 7 GB usando *wget* para transferir arquivos via HTTP.

Figura 6. Transferência de um arquivo de 7 GB usando wget

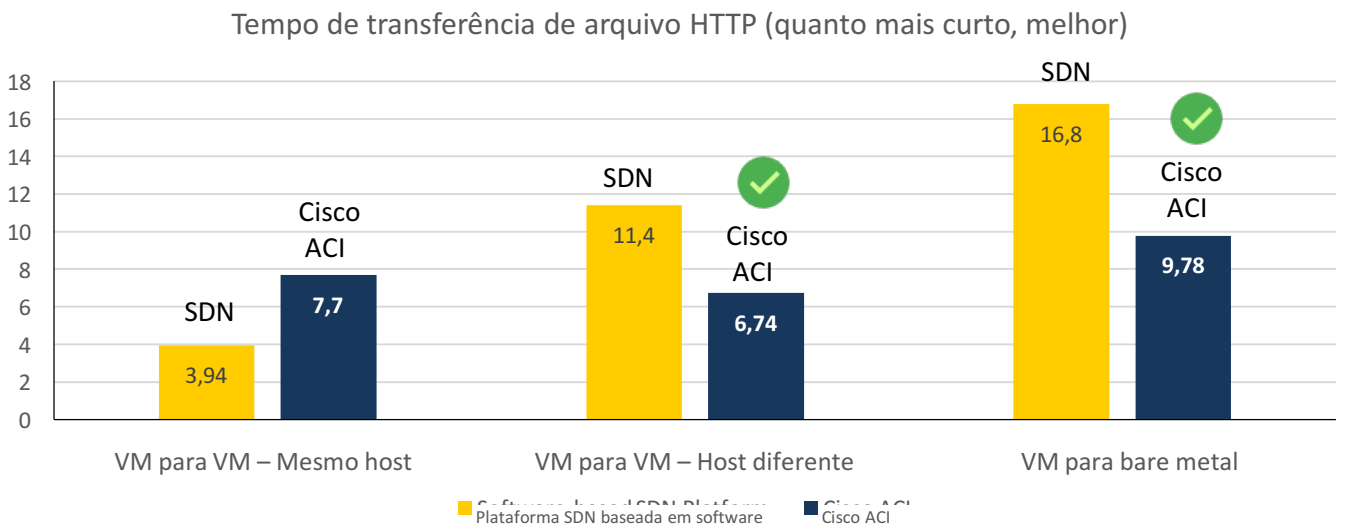


Figura 6 mostra que, embora a solução somente de software pudesse transferir arquivos entre VMs no mesmo host mais rapidamente, a ACI forneceu melhor desempenho para transferências entre hypervisors ou para servidores bare metal.

Por que isso é importante?

Redes com alto desempenho de forma constante são essenciais para a computação corporativa moderna. Todos os aspectos da empresa são afetados pelo funcionamento e pela integridade da rede, à medida que funcionários e clientes acessam dados e aplicativos de vários locais, em vários dispositivos. Quando pedimos para indicar os maiores desafios que as equipes de rede enfrentam hoje, quase um em cada quatro citou o fornecimento de desempenho de rede. A maximização do desempenho dos aplicativos foi citada por 23% dos entrevistados como um recurso que teria maior impacto ajudando as empresas a expandir seus negócios.[4]

Por meio de testes práticos, o laboratório de ESG descobriu que a Cisco ACI oferecia desempenho consistentemente melhor do que um SDN somente de software, em que as funções de roteamento e gateway de sobreposição eram fornecidas em máquinas virtuais. A ACI forneceu de 40% a 50% menor latência em testes entre VMs em diferentes hosts ESXi e até 80% menor latência entre VMs e servidores bare metal.

Embora a solução somente de software proporcionasse uma produtividade bruta mais alta entre as VMs no mesmo host, é importante observar que, em aplicativos reais, a maior parte do tráfego será entre VMs em hosts diferentes ou de VMs para servidores bare metal. A Cisco afirma que o uso de NICs de 25 GbE eliminará o gargalo, e o desempenho da comunicação de VM para VM nos mesmos hosts será comparável. Para cargas de trabalho entre VMs em hosts ESXi diferentes, a ACI oferecia uma produtividade comparável, e entre VMs e servidores bare-metal, a ACI oferecia uma produtividade 33% maior.

Para transferências de arquivos, o tipo de aplicativo teve um impacto nos resultados das VMs no mesmo hypervisor, mas quando o tráfego precisou atravessar hypervisors ou chegar a servidores bare metal, a ACI forneceu tempos de transferência consistentemente melhores.

Em ambientes reais simulados, nos quais os fluxos de tráfego são dinâmicos e muitas vezes imprevisíveis, fluindo pelo ambiente e envolvendo aplicativos e sistemas virtualizados e não virtualizados, a ACI fornece consistentemente menos latência e melhor produtividade, com desempenho previsível apropriado para aplicativos de missão crítica.

Disponibilidade de rede

Para empresas modernas, sempre em atividade, os planos de recuperação de desastres e continuidade dos negócios são de extrema importância, devido aos altos custos do tempo de inatividade. O laboratório do ESG examinou a disponibilidade na arquitetura da Cisco ACI em comparação com um SDN somente de software executado em máquinas virtuais.

O ESG estava interessado em testar a natureza ativa-ativa da ACI e observar os tempos de convergência que os usuários podem esperar em relação aos vários vetores de falha das diferentes arquiteturas e abordagens. Examinar a arquitetura de ACI revela apenas seis vetores de falha fundamentais. O ESG testou esses vetores de falha e documentou o impacto tanto da falha quanto da recuperação em Tabela 1.

[4] Fonte: Pesquisa do ESG, *Network Modernization Trends*, julho de 2017.

Tabela 1. Vetores de falha da ACI

Vetor de falha	Modo de redundância	Impacto na falha	Impacto na recuperação
Falha de nó APIC	cluster de expansão	nenhum	nenhum
Falha no cluster APIC	nó de hot standby	perda de acesso ao plano de gerenciamento	nenhum, com um backup de configuração
falha de nó do spine	ECMP	inferior a um segundo	nenhum
falha de nó do leaf	ECMP, vPC	inferior a um segundo	nenhum
falha no link de leaf/spine	ECMP, vPC	inferior a um segundo	nenhum
Falha no link do servidor	vPC	inferior a um segundo (depende da pilha de servidor)	dependente da pilha de servidor

A falha em um nó APIC e até mesmo em todo o cluster teve impacto zero no desempenho, na microssegmentação ou no roteamento SDN. Todas as outras falhas tiveram impacto inferior a um segundo. O laboratório do ESG também examinou a arquitetura da plataforma de SDN somente de software e encontrou vetores de falha adicionais com base na configuração de máquinas virtuais como roteadores e gateways de sobreposição.

Tabela 2. Vetores de falha de solução SDN somente de software

Vetor de falha	Modo de redundância	Impacto na falha	Impacto na recuperação
Gerenciamento de VM	nenhum (depende de hypervisor HA)	plano de gerenciamento, firewall	nenhum, com um backup de configuração
controlador de falha de VM	cluster de expansão	nenhum	nenhum
falha no cluster de controlador	vSphere HA, SRM	perda de acesso ao plano de gerenciamento, perda de supressão de ARP	nenhum, com um backup de configuração
falha de VM única do controle do roteador de sobreposição	HA (heartbeat)	30 a 32 segundos de tempo de inatividade	nenhum
falha de VM dupla do controle do roteador de sobreposição	nenhum (vSphere HA)	interrupção total	nenhum
modo ativo/de espera de gateway	ESG HA (heartbeat)	24 segundos de tempo de inatividade	nenhum
gateway modo ativo/ativo	ECMP	24 segundos de tempo de inatividade	até 12 segundos
falha de nó de spine subjacente	ECMP	inferior a um segundo (depende da subjacência)	nenhum
falha de nó de leaf de subjacência	ECMP, vPC	inferior a um segundo (depende da subjacência)	nenhum
falha de link de leaf/spine de subjacência	ECMP, vPC	inferior a um segundo (depende da subjacência)	nenhum
falha no link do servidor	vPC	inferior a um segundo (depende da pilha de servidor)	depende da pilha de servidor

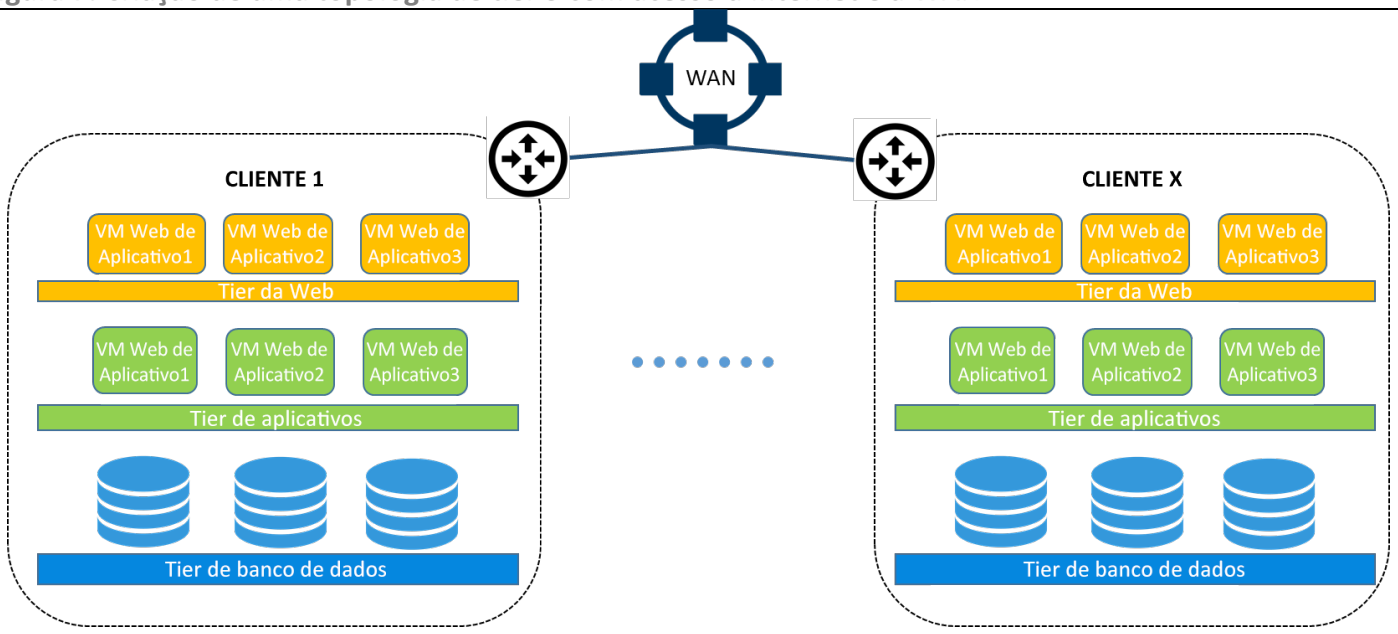
Nos testes, o laboratório do ESG detectou falhas de 24 segundos, quando um único nó de gateway falhou até uma interrupção completa da rede de sobreposição de SDN, e várias VMs do roteador de sobreposição falharam. Os resultados dos testes estão detalhados na Tabela 2. Os vetores de falha que não têm equivalente aproximado na ACI estão destacados em vermelho. Vale a pena observar que alguns desses cenários também se aplicam à manutenção planejada. Com base nessa análise, o laboratório do ESG concluiu que a Cisco ACI expõe menos vetores de falha do que a solução somente de software testada, e esses vetores de falha têm um impacto muito menor no ambiente.

Automação de rede

O laboratório do ESG também analisou as opções de automação para ACI. A automação de rede é um capacitador fundamental de valor para as tecnologias de SDN. A automação pode acelerar a entrega de serviços baseados em rede e, ao mesmo tempo, reduzir custos. A automação de rede abstrai informações de configuração para serviços de rede na infraestrutura física, o que permite que os usuários configurem serviços com ferramentas de orquestração de software automatizadas.

A ACI comporta uma ampla variedade de ferramentas de automação/orquestração, incluindo Cisco UCS-D, Cisco Cloud Center, VMware vRealize Automation/Orchestrator, Microsoft Windows Azure Pack, OpenStack Neutron (distribuições múltiplas), Ansible, Python SDK e o kit de ferramentas ACI. O laboratório do ESG usou o Ansible[5] para automatizar a criação de uma topologia de tier 3 com acesso à Internet/WAN em ambientes de ACI e SDN somente de software para qualquer número de aplicativos ou locatários, como ilustrado em Figura 7. Para essa configuração, cada cliente obtém suas próprias sub-redes roteáveis, os clientes devem ser isolados uns dos outros, a sub-rede da Web deve ser anunciada automaticamente para o dispositivo WAN, as conexões para sub-redes bare metal devem ser automáticas e o controle de rede e o plano de dados devem ser redundantes.

Figura 7. Criação de uma topologia de tier 3 com acesso à Internet e à WAN



Fonte: Enterprise Strategy Group, 2017.

Houve vários desafios na implementação desse cenário com o SDN somente de software, incluindo alguns itens que não puderam ser automatizados e uma etapa que exigiria que o engenheiro de DevOps entendesse o suficiente sobre roteamento para criar rotas estáticas dos gateways do locatário para OSPF, uma perspectiva complexa. A implantação de dez topologias para SDN somente de software levou cerca de 60 minutos para concluir. Além disso, os roteadores e

[5] Você pode encontrar os módulos de Ansible da Cisco ACI aqui: http://docs.ansible.com/ansible/devel/list_of_network_modules.html#aci

gateways baseados em VM exigiam 40 vCPU, 30 GB de RAM e 60 GB de armazenamento. A implantação da ACI exigiu zero de experiência em roteamento, automatizou todas as atividades, exigiu 20% menos linhas de código e a implantação de dez topologias concluídas em apenas 1,5 minuto. Não houve novos recursos necessários para a implantação da ACI.

Por que isso é importante?

Em ambientes modernos com recursos e mão de obra altamente distribuídos, a disponibilidade da rede é essencial para os negócios e para a missão. Se a rede falhar, tudo falhará. À medida que as redes se expandem para lidar com os negócios de escala da Web atuais, elas se tornam mais complexas e difíceis de implantar e gerenciar, gerando problemas de desempenho e tempo de atividade, que frustram usuários e clientes.

A rede definida por software foi inventada para simplificar o controle e as operações de rede ao abstrair os planos de controle e dados do hardware subjacente. Com a criação de componentes de rede lógicos, programáveis e dinâmicos baseados em componentes físicos de alta qualidade, a SDN pode oferecer serviços de rede mais confiáveis e fáceis de projetar, gerenciar e solucionar problemas.

Porém, nem todas as SDNs de trabalho são criadas da mesma forma. As soluções SDN somente de software, nas quais as funções de roteamento e gateway são executadas nas VMs, podem ser problemáticas quando se trata de oferecer suporte a aplicativos essenciais que exigem convergência inferior a um segundo, como voz, vídeo ou serviços financeiros.

O laboratório do ESG validou que a Cisco ACI fornece uma SDN altamente disponível, SDN ativa-ativa, adequada para aplicativos essenciais para a missão e os negócios. A arquitetura da ACI tem menos vetores de falha, e todos os eventos de falha de rede que o ESG testou mostraram impacto no tráfego zero ou inferior a um segundo. Com a SDN somente de software, o ESG viu maior complexidade e mais vetores de falha, juntamente com até 32 segundos de inatividade em eventos de falha únicos, devido à natureza ativa-passiva da arquitetura.

O laboratório do ESG utilizou o Ansible para automatizar o provisionamento de um ambiente de nuvem privada com a ACI mais de 40 vezes mais rápido do que seria possível com o SDN somente de software. O laboratório do ESG também confirmou uma economia significativa na capacidade de computação e armazenamento, pois a ACI não exige VMs adicionais para executar serviços de roteamento e gateway.

Segurança

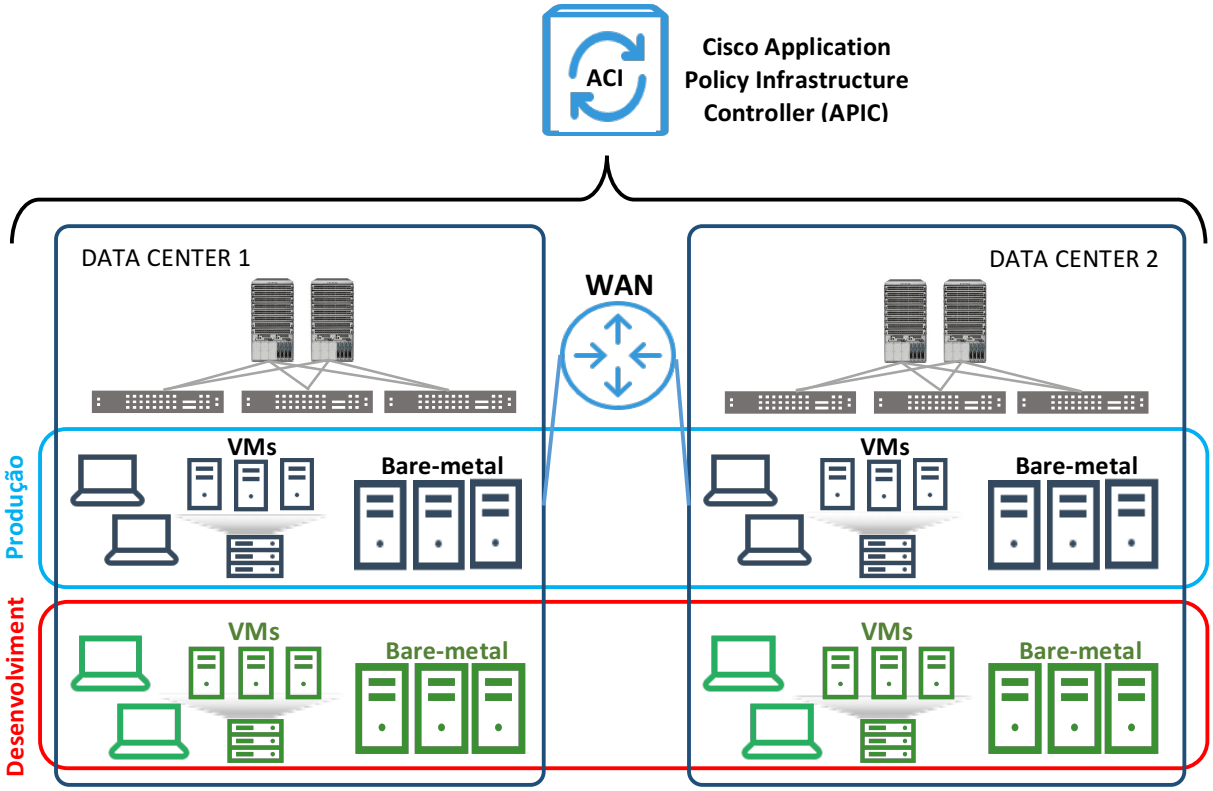
A Cisco ACI foi projetada para fornecer suporte consistente à microssegmentação para vários hypervisors, endpoints bare metal e contêineres, o que permite a imposição de segurança do endpoint granular. A microssegmentação permite que as políticas de segurança sejam aplicadas no nível de carga de trabalho, em vez de depender de outros elementos de rede (por exemplo, firewalls) para fornecer segurança de rede de ponta a ponta somente no nível de tráfego de rede. Para aprovar políticas de segurança, a Cisco ACI criará um contrato específico para cada tipo de carga de trabalho. O contrato determina os dados e os terminais que uma carga de trabalho pode acessar, independentemente de seu posicionamento no data center. Se uma carga de trabalho é movida dentro de data centers ou entre eles, a Cisco ACI mantém o contrato. Os contratos de ACI definem regras de segurança até a camada 4. Os contratos na ACI também podem definir outros parâmetros de QoS.

Teste do ESG Lab

O laboratório do ESG examinou primeiro como a Cisco ACI aplica regras de segurança de maneira consistente em cargas de trabalho localizadas em dois data centers e em diferentes vCenters. Os data centers foram conectados entre si por uma WAN roteada por IP. Figura 8 ilustra a topologia de teste. Configuramos dois clientes em sites separados de produção e desenvolvimento do WordPress em um data center. Em seguida, usamos a Cisco ACI para permitir que a microssegmentação abrangesse os data centers e aplicasse as seguintes regras de firewall:

- Permitir que o cliente de produção na WAN se comunique com os sites de produção do WordPress em ambos os data centers, evitando a comunicação com os sites de desenvolvimento.
- Permitir que o cliente de desenvolvimento na WAN se comunique com os sites de desenvolvimento em ambos os data centers, evitando a comunicação com os sites de produção.

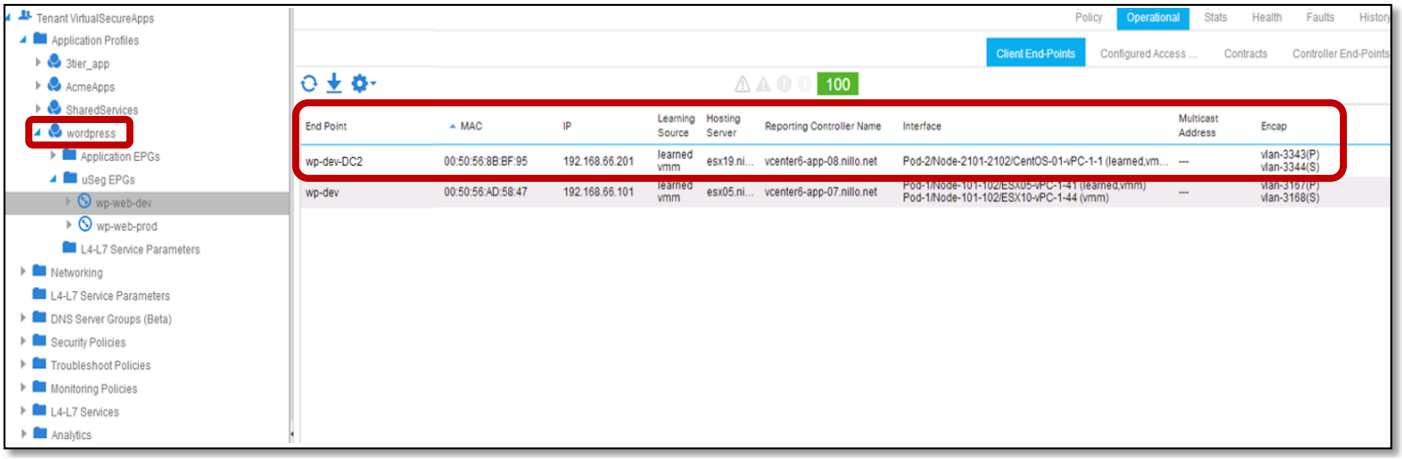
Figura 8. Topologia de laboratório: microssegmentação entre data centers



Fonte: Enterprise Strategy Group, 2017.

Extremamente importantes, as VMs foram classificadas nas políticas de segurança corretas usando objetos do vCenter, em particular uma combinação de tags do vSphere. Confirmamos então que as regras de firewall foram observadas, pois cada cliente se comunicava com os sites conforme definido em seu contrato individual. Mais importante, vimos que a Cisco ACI aplicou as mesmas regras de firewall a sites de produção e desenvolvimento em ambos os data centers, mesmo quando as VMs foram movidas em diferentes vCenters usando o vMotion. O laboratório do ESG também analisou os detalhes de VMs individuais sob microssegmentação em ambos os data centers. Os detalhes da carga de trabalho incluíam endereço IP, endereço MAC e host do servidor. Figura 9 mostra os detalhes para as VMs de desenvolvimento em ambos data centers. Além de detalhes da VM, podem ser visualizados detalhes do contrato para garantir que a Cisco ACI esteja aplicando as políticas corretas.

Figura 9. Detalhes das cargas de trabalho individuais na GUI da ACI



Fonte: Enterprise Strategy Group, 2017.

O ESG também realizou o mesmo teste com a solução SDN somente de software usando uma topologia semelhante. Observamos que, diferente da Cisco ACI, essa solução de software não conseguia manter as políticas de firewall nos dois data centers quando a VM migrava entre diferentes vCenters. Descobrimos que as políticas foram violadas ao tentar aplicar as regras de maneira consistente nos data centers.

Por que isso é importante?

Quando pedimos para indicar os recursos de rede que teriam o maior impacto em ajudar a empresa a expandir seus negócios, 46% dos entrevistados de uma recente pesquisa do ESG citaram a garantia da segurança da rede, sendo essa a resposta mais citada por ampla margem.[6]

À medida que as empresas continuam a virtualizar seus aplicativos, a execução da segurança de rede do data center torna-se cada vez mais complexa, especialmente quando as VMs podem ser movidas para diferentes hosts dentro dos data centers e entre eles. A aplicação de regras e políticas de segurança no nível da rede pode se tornar complicada, pois os profissionais de TI precisam garantir que todos os elementos na rede do data center apliquem regras e políticas consistentemente para todos os tipos de tráfego de rede. A inconsistência na aplicação de políticas pode resultar em perda de dados, vulnerabilidades de rede e interrupções não planejadas, que podem levar à erosão da marca e perda de receita.

O laboratório do ESG testou a capacidade da Cisco ACI de fornecer suporte de microssegmentação compatível com as cargas de trabalho em vários hypervisors, endpoints bare metal e contêineres, em data centers conectados por meio de uma WAN. Aplicamos um contrato a uma carga de trabalho de produção e a uma carga de trabalho de desenvolvimento, que forneceu a aplicação de segurança granular do endpoint em dois data centers. Vimos que ambas as cargas de trabalho poderiam se comunicar apenas com os sites definidos no contrato. Realizamos o mesmo teste com uma solução SDN somente de software e descobrimos que as políticas foram violadas ao tentar aplicar as mesmas políticas de firewall às mesmas cargas de trabalho nos data centers.

[6] Fonte: Pesquisa do ESG, *Network Modernization Trends*, julho de 2017.

Entrevista com o cliente

O laboratório do ESG conversou com Indranil Sengupta, chefe de Engenharia de Produto e Operações da NTT America, sobre o uso da Cisco ACI no data center em nuvem da NTT America. A NTT America atende a América do Norte, do Sul e Central como parte da NTT Communications, uma empresa global da Fortune 500. Essa divisão da NTT America fornece serviços gerenciados de infraestrutura para clientes corporativos globais com requisitos complexos.

A NTT America fornece plataformas de infraestrutura e gerenciamento contínuo para as necessidades de teste/desenvolvimento e produção. Para ser bem-sucedido neste setor competitivo, ela deve fornecer serviços confiáveis e seguros que sejam dimensionados, enquanto se concentra constantemente em melhorar a eficiência. A rede definida por software da Cisco ACI automatiza a implantação e o gerenciamento contínuo dos serviços de rede, permitindo que a NTT America gerencie com menos esforço e custo e ajuste os serviços de maneira rápida e fácil à medida que as necessidades dos clientes mudam e aumentam.

Os multi-inquilinos são essenciais para manter as plataformas de serviço gerenciado econômicas, mas devido à complexidade das necessidades dos clientes da NTT America, cada infraestrutura de locatário é diferente. Os serviços da Web de hiperescala típicos comportam multi-inquilinos usando uma abordagem de cookie, com todos os serviços essencialmente iguais - não uma opção com os requisitos complexos dos clientes da NTT America. A Cisco ACI permite aproveitar a eficiência de multi-inquilino, ao mesmo tempo em que fornece redes sob medida para cada cliente. Sem a Cisco ACI, os engenheiros da NTT America precisariam criar individualmente cada ambiente de locatário, incômodo para os clientes e caro para a NTT America.

Com a Cisco ACI, a NTT America pode escalar com mais facilidade a entrega de serviços, reduzindo custos. A Cisco ACI também permitiu que a empresa reduzisse o tempo de serviço. "Implantamos uma solução para um cliente financeiro; era complexo, com conformidade rigorosa e parâmetros de segurança", comentou Sengupta. "A Cisco ACI nos permitiu implantá-lo na metade do tempo esperado e o cliente ficou muito satisfeito."

A NTT America planeja continuar expandindo sua implantação da Cisco ACI para mais clientes e aproveitando a maior eficiência e flexibilidade oferecidas. Afirmou Sengupta, "É um setor muito competitivo, então a cada trimestre precisamos de mais melhorias na redução de esforços e custos. Com a Cisco ACI, podemos fornecer mais e melhores serviços aos clientes sem aumentar o preço."

A grande verdade

Acompanhar o ritmo e a escala da empresa atualmente exige muito da TI. Os administradores estão sobrecarregados até o limite, geralmente lidando com centenas de aplicativos com requisitos diferentes, bem como usuários em vários locais com vários terminais. Além disso, a consumerização de TI fez com que os usuários tivessem expectativas mais altas, além de atitudes aprimoradas. Nesse contexto, uma solução SDN sofisticada não é apenas uma "boa pedida", mas sim uma base de negócio bem-sucedida e lucrativa. A simplicidade operacional e os recursos de automação serão inúteis se não forem corroborados por um alto desempenho constante. Uma experiência de cliente superior e ininterrupta exige um ecossistema altamente disponível e "sempre conectado" para aplicativos modernos que comportam aplicativos de missão crítica e sensíveis à produtividade e à latência, como vídeo, voz e serviços financeiros. Para fornecer um modelo de segurança viável, uma solução SDN deve vincular e proteger aplicativos em vários data centers, tanto vertical quanto horizontalmente.

À medida que mais empresas buscam adotar o movimento da nuvem híbrida e expandir a execução de aplicativos nos domínios locais e em várias nuvens, elas precisam mudar do gerenciamento focado em infraestrutura para o gerenciamento centrado em aplicativos, visando aproveitar os modernos sistemas de TI, incluindo serviços e tecnologias de nuvem pública, tais como contêineres e microsserviços. Isso não significa que o gerenciamento de infraestrutura não seja mais importante, mas mostra que o foco da nuvem híbrida é a abstração da infraestrutura subjacente aos aplicativos de suporte. À medida que as empresas continuam a utilizar novas tecnologias para sustentar suas transformações de TI, a nuvem híbrida se tornará uma tecnologia impulsionadora, e uma sólida estratégia de SDN para dar suporte a esses aplicativos dinâmicos é um requisito para um plano de nuvem híbrida bem-sucedido.

A Cisco ACI oferece essa solução, criando um ecossistema que fornece serviços de rede com foco em aplicativos para se obter eficiência, simplicidade, segurança, alto desempenho e alta disponibilidade. Inclui elementos físicos, virtuais e de nuvem, e é facilmente escalável com o ambiente crescente de uma empresa. Utilizando a rede definida por software de um cluster de controlador e switches de Nexus 9000 Series, a Cisco ACI descobre e gerencia a estrutura de rede em vários hypervisors e data centers, e a sua estrutura aberta facilita a integração com soluções de fornecedores de gerenciamento de rede e orquestração.

O ESG validou que a ACI oferecia um desempenho constante e de alto desempenho que se traduz em ambientes do mundo real, nos quais os fluxos de tráfego são dinâmicos e muitas vezes imprevisíveis, envolvendo aplicativos e sistemas virtualizados e não virtualizados. Nos testes do ESG, a ACI forneceu consistentemente menor latência e melhor rendimento, com desempenho previsível apropriado para aplicativos de missão crítica. O laboratório do ESG validou que a Cisco ACI fornece uma SDN altamente disponível, adequada para aplicativos essenciais para a missão e os negócios. Todos os eventos de falha de rede que o ESG testou não tiveram impacto no tráfego ou tiveram um impacto inferior a um segundo.

O laboratório do ESG utilizou o Ansible para automatizar o provisionamento de um ambiente de nuvem privada com a ACI mais de 40 vezes mais rápido do que seria possível com um SDN somente de software. O laboratório do ESG também confirmou uma economia significativa na capacidade de computação e armazenamento, pois a ACI não exige VMs de infraestruturas adicionais para executar serviços de roteamento e gateway. O ESG também validou que a Cisco ACI pode aplicar políticas de microssegmentação e segurança de forma consistente dentro e entre os data centers.

As empresas são cada vez mais desafiadas a construir redes que possam responder às necessidades de negócios de data centers e nuvens públicas e privadas altamente virtualizados, com uma combinação de infraestrutura virtualizada e física. O ESG descobriu que a Cisco ACI fornece uma rede simples, escalonável e altamente disponível que é adequada às cargas de trabalho de missão crítica. Se a empresa estiver interessada em melhorar a automação, a agilidade, a segurança e a disponibilidade das redes em vários data centers híbridos, o laboratório do ESG recomenda uma análise mais detalhada da Cisco ACI.

O Enterprise Strategy Group é uma empresa de análise, pesquisa, validação e estratégia de TI que fornece inteligência e informações práticas sobre o mercado à comunidade global de TI.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188