Cisco Intercloud Fabric: 선택, 일관성, 제어 및 규정준수를 지원하는 하이브리드 클라우드

2015년 9월 8일

Cisco Intercloud Fabric: 선택, 일관성, 제어 및 규정준수를 지원하는 하이브리드 클라우드

목차

1 장

소개

이 문서는 하이브리드 구축을 위한 아키텍처 결정을 내리는 IT 의사 결정권자, 설계자, 엔지니어 및 애플리케이션 소유자를 위해 작성되었습니다. 이 문서에 설명된 아키텍처는 하이브리드 클라우드 솔루션을 고려 중인 대기업과 중견기업을 위한 것입니다. 이 문서는 기업에 하이브리드 클라우드 서비스를 제공하는 서비스 사업자에도 유용합니다.

하이브리드 클라우드 환경 및 과제

2012년 12월에 Cisco는 Forrester Consulting에 의뢰하여 날로 주목받고 있는 IaaS(infrastructure as a service), 특히 하이브리드 클라우드 모델에 대해 조사했습니다. Forrester에 따르면 미국과 유럽의 엔터프라이즈 IT 의사 결정권자 중 절반가량이 자사에서 클라우드 IaaS를 사용하고 있다고 대답했으며, IaaS를 채택하는 기업이 점차 늘어날 것으로 전망된다고 합니다. 프라이빗 클라우드를 채택 중인 대부분의 기업에서 온프레미스 인프라가 계획되지 않은 성장을 해결하는 데 필요한 리소스를 제공하지 못하는 경우도 있습니다. 하이브리드 클라우드 아키텍처는 프라이빗 클라우드 인프라와 클라우드 서비스 사업자 인프라가 결합된 것으로 사용자에게 퍼블릭 클라우드의 무제한 리소스와 프라이빗 클라우드에서 관리되는 보안 및 제어 기능을 제공합니다.

IT 의사 결정권자들이 하이브리드 클라우드의 IaaS에서 가장 관심을 보이는 부분은 온프레미스 용량을 대체하는 것이 아니라 보완하는 것이라고 합니다. 의사 결정권자들은 결과적으로 네트워크 운영과 지출에 영향을 줄 수 있는 계획을 준비하고 있습니다. 하이브리드 방식을 사용하면 비용을 절감하고 IT 및 비즈니스의 유연성을 크게 강화할 수 있지만, 하이브리드 클라우드 아키텍처 내의 클라우드 서비스에서 온프레미스 인프라를 관리하고 통합하는 데 약간의 문제점이 있습니다.

Forrester에서는 미국, 영국, 프랑스 및 독일에 있는 69명의 IT 의사 결정권자를 대상으로 클라우드 전략에 대해 질문했습니다. 이들은 클라우드 IaaS 서비스 사업자를 이용하는 데 관심이 있거나 이미 이용하고 있었으며, 대부분(76%)이 하이브리드 클라우드를 구현할 계획이라고 합니다. 또한 2012 Gartner Data Center Summit 설문조사에서는 2015년이 되면 엔터프라이즈의 70%가 하이브리드 클라우드 전략을 채택할 것으로 예상했습니다. 하이브리드 클라우드를 채택한 대부분의 업체에서는 IaaS를 온프레미스 서버 및 스토리지를 보완하기 위해 사용할 계획이지만, 많은 수가 최대 워크로드 및 기타 활용 사례에 알맞은 서비스 사업자를 모색하고 있었습니다.

또한 IaaS를 사용 중인 회사의 의사 결정권자들에 따르면 하이브리드 클라우드 전략의 가장 중요한 이점은 IT 유연성, 비용 절감, 시장 및 비즈니스 요구 사항에 대한 더 빠르고 유연한 대처라고 합니다. IT 의사 결정권자들은 하이브리드 클라우드 전략과 관련된 잠재적인 문제점에 대해서도 정확히 알고 있습니다. 대부분은 데이터 센터와 클라우드 서비스 사업자를 아우르는 고도의 보안 통신과 일관된 보안 정책을 원하고 있으며, 두 위치 모두에서 기존 애플리케이션이 어떻게 작동하는지를 알고 싶어 합니다. 다른 중요한 요구 사항으로는 가상 머신의 이동을 위한 클라우드 서비스 사업자와의 투명한 통합, 클라우드 서비스 사업자와 네트워크 공유, 하이브리드 클라우드 아키텍처 전반에서 일관된 애플리케이션 관리 등이 있습니다.

IT 의사 결정권자들은 기존 툴과 기술을 사용하여 이러한 문제에 대한 솔루션을 찾거나, 하이브리드 클라우드 전략의 과제를 보다 쉽게 해결할 수 있는 새로운 제품을 찾을 것입니다. 최신 솔루션은 다음과 같이 가장 시급한 하이브리드 클라우드 과제를 해결할 수 있습니다.

- 방화벽, 보안 및 애플리케이션 제공에 대한 일관된 정책 시행 및 기능
- 가상 머신 마이그레이션을 위한 고도의 보안 네트워크 연결성
- 데이터 센터 및 클라우드 서비스 사업자 전반에 걸쳐 워크로드 및 리소스 보기
- 이기종 하이퍼바이저 환경 및 인프라 소프트웨어 지원
- 워크로드 모빌리티 및 이식성

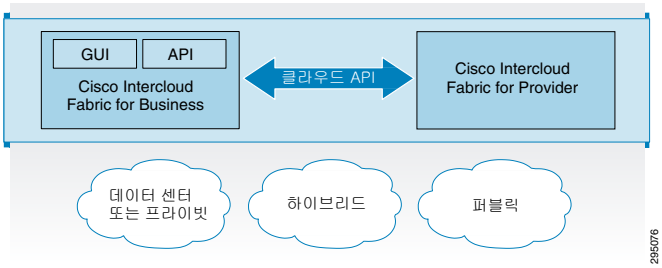
Cisco Intercloud Fabric 개요 및 가치 제안

Cisco Intercloud Fabric 소프트웨어 솔루션을 사용하는 고객은 이기종 환경의 여러 퍼블릭 클라우드를 통해 워크로드를 관리 및 액세스하여, 기술(용량, 보안 등) 또는 비즈니스(규정준수 등) 요구 사항에 따라 가장 유리한 위치에 워크로드를 유연하고 자유롭게 배치할 수 있습니다.

또한 퍼블릭 클라우드로 안전하게 확장할 수 있는 네트워크를 선택하고, 하이브리드 클라우드 전체에서 일관된 네트워크 구성 및 보안 정책을 시행할 수 있습니다. Intercloud Fabric의 보안 시행 메커니즘은 프라이빗 클라우드와 퍼블릭 클라우드 사이의 보안 터널뿐만 아니라 클라우드에서 실행 중인 VM(Virtual Machine)에도 보안을 적용하므로 클라우드 내의 VM 간 통신에 보안이 적용될 수 있습니다. 이 메커니즘은 이 문서의 뒷부분에서 설명합니다.

그림 1-1에서는 이기종 환경의 프라이빗 클라우드에서 Cisco Intercloud Fabric for Business를 구축할 수 있는 엔터프라이즈 고객을 위한 솔루션 공간을 보여 줍니다. 이 소프트웨어 솔루션에는 IT 조직에서 워크로드, 보안 정책, 클라우드로의 네트워크 확장 등을 관리할 수 있는 관리 포털을 제공하며, 기존 프라이빗 클라우드 관리 솔루션과 통합할 수 있는 노스바운드(Northbound) API 기능이 있습니다. 엔터프라이즈 LOB(lines of businesses)를 비롯한 IT 고객은 Intercloud Fabric for Business 내장형 셀프 서비스 카탈로그를 활용하여 여러 클라우드에서 새로운 워크로드를 만들고, 엔드 유저 포털을 통해 워크로드 라이프사이클 및 마이그레이션을 관리할 수 있습니다.

그림 1-1 Cisco Intercloud Fabric 솔루션



Cisco Intercloud Fabric for Provider는 Intercloud Fabric 에코시스템의 일부인 클라우드 사업자가 설치 및 관리하는 멀티 테넌트 소프트웨어 어플라이언스입니다. 가상 어플라이언스를 사용하면 다양한 클라우드 사업자 간에 균일한 클라우드 API를 구축하고 이기종 클라우드 API 지원의 복잡성을 추상화할 수 있습니다. 향후 Intercloud Fabric for Provider를 사용하면 모든 Cisco Powered Cloud Providers를 Cisco 인프라별로 차별화할 수 있습니다.

Cisco Intercloud Fabric을 사용하는 고객은 Cisco Powered Cloud Providers 에코시스템과 하이퍼스케일 퍼블릭 클라우드(예: Amazon EC2 및 Microsoft Azure)를 비롯한 다양한 클라우드 사업자를 선택할 수 있습니다. 또한 기업 고객은 가상화된 환경에 하이퍼바이저를 사용하려고 하므로,

하이브리드 클라우드가 하이퍼바이저에 종속되지 않도록 지원하는 솔루션이 필요합니다. 온프레미스와 오프프레미스에서 여러 하이퍼바이저를 선택하는 시나리오에서 워크로드 모빌리티 및 이식이 어려울 수 있지만, Cisco Intercloud Fabric을 사용하면 이 문제를 해결하는 한편 고객이 투명하게 확인할 수 있으므로 워크로드를 여러 클라우드로 이동할 수 있으며 나중에 다시 엔터프라이즈로 가져올 수도 있습니다.

요약하면 Cisco Intercloud Fabric은 비즈니스 요구 사항에 더 유연하게 대응하고 하이브리드 클라우드의 잠재적인 과제를 해결하는 것을 목표로 하며, 아래와 같은 이점을 제공합니다.

- 결과물인 하이브리드 클라우드 전반에서 워크로드 보안 실현
- 클라우드 전체에서 일관된 운영 및 워크로드 모빌리티 Cisco Intercloud Fabric에서는 엔드 유저와 IT 관리자에게 통합형 하이브리드 클라우드 관리 기능을 제공하여, 물리 및 가상 워크로드에 대해 서비스 사업자 클라우드 간의 워크로드 모빌리티를 지원합니다.
- 중요 비즈니스 자산을 보호하고 규정준수 요구 사항을 충족하기 위해 Cisco Intercloud Fabric에서는 프라이빗 클라우드를 서비스 사업자 클라우드로 확장할 때 매우 안전하고 확장성이 뛰어난 연결을 제공합니다.

Cisco Intercloud Fabric 활용 사례

Cisco의 업계 연구에 따르면 하이브리드 클라우드 설계의 가장 일반적인 활용 사례는 개발 및 테스트, 용량 확장, 새도우(비인가) IT 제어입니다. Cisco Intercloud Fabric 로드맵을 사용하면 재해 복구 지원을 추가할 수 있습니다.

개발 및 테스트

개발 및 테스트 활용 사례에서 엔터프라이즈 고객은 서비스 사업자 클라우드에서 워크로드를 개발하고, 워크로드가 프로덕션 환경으로 승격된 이후에 프라이빗 클라우드로 다시 가져옵니다. 클라우드의 경제적 이점을 실현하고 더 빠른 개발을 지원하기 위해 많은 애플리케이션 개발자들은 개발 및 테스트 환경에 서비스 사업자 클라우드를 사용합니다.

하지만 서비스 사업자 클라우드에서 프로덕션 애플리케이션을 배포할 경우 IT 부서에 심각한 보안 및 규정준수 문제가 발생합니다. IT 의사 결정권자는 애플리케이션 개발자에게 유연성을 제공하여 클라우드 서비스 사업자를 이용할 수 있도록 지원하려고 하지만, PCI(Payment Card Industry), HIPAA(Health Insurance Portability and Accountability Act), Sarbanes-Oxley 규정 등과 같은 규정준수 요구 사항을 충족하는 보안 및 제어 기능을 갖춘 프라이빗 클라우드에서 프로덕션 워크로드를 구축해야 합니다. Cisco Intercloud Fabric은 워크로드를 서비스 사업자 클라우드로 이동하고 고객의 프라이빗 클라우드 및 온프레미스 인프라로 다시 가져올 수 있는유연성을 제공합니다.

용량 확장

용량 확장 활용 사례에서는 임시 리소스에 대한 필요성을 해결합니다. 예를 들어, 기업에서는 계절적 수요를 충족하기 위해 서비스 사업자 클라우드를 통해 임시 리소스를 제공할 수 있습니다. 이 경우 높은 수요가 완전히 처리되면 리소스를 해제합니다. 예를 들어, 소매업체의 경우 최대 쇼핑 시즌이나 금융 서비스의 세무 신고 기간에는 추가 클라우드 리소스에 대한 계획되거나 계획되지 않은 장단기적 수요가 발생합니다. 하이브리드 클라우드의 경제적 이점을 실현하기 위해 고객은 프라이빗 클라우드의 보안 및 제어 이점을 유지하면서 최대 수요에 맞게 서비스 사업자 클라우드로 유연하게 확장할 수 있습니다. Cisco Intercloud Fabric 솔루션은 프라이빗 클라우드의 보안성과 제어력뿐만 아니라 필요한 용량을 투명하게 제공합니다.

섀도우 IT 제어

대부분의 기업에서는 대개 편리하고 더 빠른 구축을 위해 퍼블릭 클라우드에서 개발 워크로드를 구축하는 것을 선호합니다. 이 방법은 IT 트래픽 플로우와 지출을 제어하고 데이터 및 지적 재산권에 대한 보안을 보장해야 하는 IT 관리자에게 문제가 될 수 있습니다. 적절한 제어가 없다면 데이터와 지적 재산권이 감독에서 벗어날 수 있습니다. Cisco Intercloud Fabric 솔루션을 사용하면 IT의 제어를 벗어난 퍼블릭 클라우드에 구축된 리소스를 검색하여(부록 A, "섀도우 IT 및 Cisco Cloud Consumption Professional Services") Cisco Intercloud Fabric의 통제하에 두어 섀도우 IT를 제어할 수 있습니다.

Intercloud Fabric 구축 모델

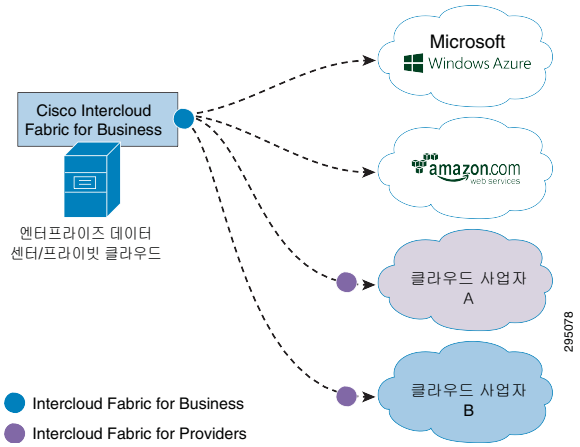
Cisco Intercloud Fabric은 두 하이브리드 클라우드 구축 모델(엔터프라이즈 매니지드 및 서비스 사업자 매니지드)에 적합한 클라우드 구축 요구 사항을 해결합니다.

엔터프라이즈 매니지드

엔터프라이즈 매니지드 하이브리드 클라우드 구축 모델에서 기업은 자체 클라우드 환경을 관리합니다. Cisco Intercloud Fabric에서는 엔터프라이즈 IT 부서에 프라이빗 클라우드와 퍼블릭 클라우드 모두에 대한 관리 권한을 부여하면서 프라이빗 클라우드를 퍼블릭 클라우드로 확장하는 하이브리드 클라우드 시나리오를 사용합니다.

이 하이브리드 클라우드 시나리오에서 기업은 서비스 사업자와 계약을 맺고, 서비스 사업자는 기업에서 사용할 일부 클라우드 리소스(컴퓨팅, 스토리지, 네트워크 연결성)를 제공합니다. 기업에서는 Cisco Intercloud Fabric 솔루션을 사용하여 네트워크를 퍼블릭 클라우드로 투명하고 안전하게 확장함으로써 온프레미스 프라이빗 클라우드에서와 같은 방법으로 퍼블릭 클라우드의 리소스를 취급하고 처리할 수 있습니다. 모든 보안 및 정책 요구 사항은 하이브리드 클라우드 전체에 적용됩니다(그림 1-2).

그림 1-2 엔터프라이즈 매니지드 하이브리드 클라우드



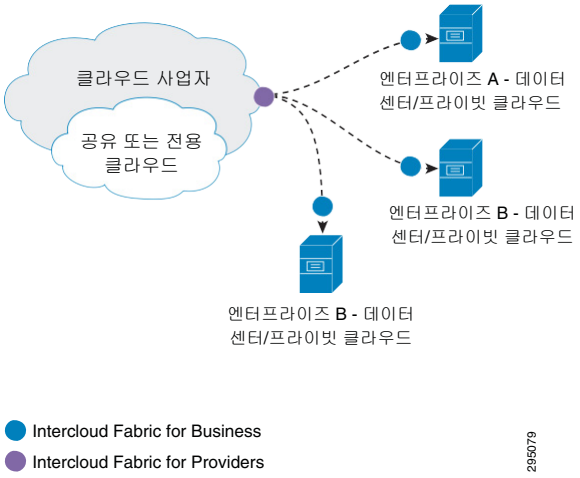
서비스 사업자 매니지드

서비스 사업자 매니지드 하이브리드 클라우드 시나리오에서는 서비스 사업자가 모든 클라우드 리소스를 관리 및 제어합니다. 서비스 사업자의 고객은 서비스 사업자 매니지드 클라우드에서 리소스를 사용하고 워크로드를 구축하지만, 전체 클라우드 환경에 대한 관리 권한은 서비스 사업자에 있습니다.

이 시나리오에서 고객은 데이터 센터를 운영하는 데 집중할 필요가 없으며, 새로운 애플리케이션 및 기술을 시장에 더 빠르게 출시하는 데 주력할 수 있습니다.

이 시나리오에서도 하이브리드 클라우드를 구축해 사용할 수 있습니다. Cisco Intercloud Fabric에서는 프라이빗 클라우드 환경(일반적으로 VPC[Virtual Private Cloud])과 다양한 퍼블릭 클라우드를 투명하고 매우 안전하게 연결할 수 있습니다(그림 1-3).

그림 1-3 서비스 사업자 매니지드 하이브리드 클라우드



신규 구축

Cisco Intercloud Fabric 솔루션은 퍼블릭 클라우드를 채택의 초기 단계에 있지만 아직 단계를 완료하지 않은 조직에 상당히 유리합니다. Cisco Intercloud Fabric 솔루션을 사용하면 프라이빗 클라우드와 퍼블릭 클라우드 간의 워크로드 마이그레이션을 보다 안전하게 관리하고 클라우드 간 정책 일관성을 지원할 수 있습니다.

기존 구축

개발자가 이미 IT를 우회하여 퍼블릭 클라우드 솔루션을 구축한 조직에서는 Cisco Cloud Consumption 서비스(부록 A, "새도우 IT 및 Cisco Cloud Consumption Professional Services")를 사용하여 퍼블릭 클라우드 사용을 식별하고 IT와 개발자 간의 협업을 복원할 수 있습니다. 이러한 조직에서 고려할 수 있는 방법은 다음과 같습니다.

- Cisco Cloud Onboarding 서비스를 사용하여 조직의 규정준수 요구 사항을 충족할 수 있는 서비스 사업자에 워크로드를 마이그레이션합니다. 이러한 서비스는 대량 구매 혜택을 제공하므로 공통된 권한에 따라 모든 IT 비용을 관리하고 가용성 및 비즈니스 연속성 요구 사항을 충족합니다.

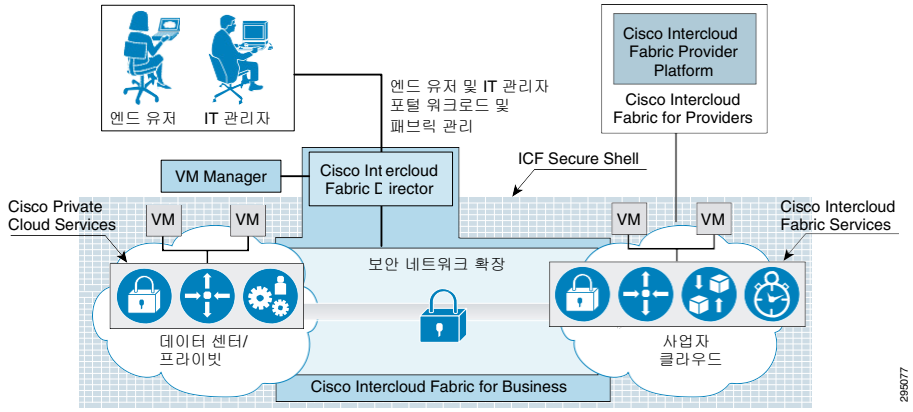
- Cisco Intercloud Fabric을 구축하여 워크로드를 IT 관리로 되돌리고 솔루션을 조직의 기존 인프라 및 툴과 통합합니다. 이 방식은 간단하면서 매우 안전한 하이브리드 클라우드 통합 계획을 지원합니다.
- Cisco Cloud Consumption 서비스를 계속 사용하여 퍼블릭 클라우드 사용을 추적합니다.

2장

Cisco Intercloud Fabric 아키텍처 개요

그림 2-1에서는 Cisco Intercloud Fabric 아키텍처의 개요를 설명합니다.

그림 2-1 Cisco Intercloud Fabric 솔루션 개요



Cisco InterCloud Fabric 아키텍처에서는 다음과 같은 두 가지 소비 모델을 충족하는 두 가지 제품 구성을 제공합니다.

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers

Cisco Intercloud Fabric for Business

Cisco Intercloud Fabric for Business는 전체 환경에서 동일한 수준의 보안 및 정책을 유지하면서 프라이빗 클라우드를 퍼블릭 클라우드 환경으로 투명하게 확장하려는 엔터프라이즈 고객에게 알맞습니다. Cisco Intercloud Fabric for Business는 다음 구성 요소로 이루어져 있습니다.

- Cisco Intercloud Fabric Director
- Cisco Intercloud Fabric Secure Fabric

Cisco Intercloud Fabric Director

하이브리드 환경에서 워크로드 관리는 프라이빗 또는 퍼블릭 및 사업자 클라우드와 네트워크 확장에서 가상 서비스를 구축하여 관리하는 기능에 국한되지 않습니다. 두 기능은 모두 전체 하이브리드 클라우드 솔루션의 일부이며 정책 기능(배치, 할당량 등), 이기종 환경의 워크로드 관리 기능, 여기에 설명된 기타 기능 등과 같은 다양한 유형의 서비스를 제공해야 합니다.

Cisco ICFD(Intercloud Fabric Director)는 엔드 유저와 IT 관리자에게 여러 클라우드에서 워크로드를 구축 및 관리할 수 있는 원활한 환경을 제공합니다. 이 환경은 하이브리드 클라우드 솔루션을 위한 단일 관리 및 소비 지점이 됩니다.

이기종 클라우드 플랫폼은 프라이빗 클라우드에 있는 Cisco ICFD에 의해 지원되며, 운영 면에서 VMware vSphere 및 vCloud, Microsoft Hyper-V 및 SCVMM(System Center Virtual Machine Manager), OpenStack, CloudStack 등과 같은 다양한 클라우드 인프라 플랫폼으로 구성된 클라우드 내에서 워크로드 관리를 통합합니다. 통합을 통해 고객의 클라우드 인프라 플랫폼에 종합적인 워크로드 관리 환경과 다양한 옵션을 제공합니다. Cisco ICFD는 다양한 클라우드 인프라 플랫폼과 통합하는 데 필요한 SDK(Software Development Kit) 및 API를 제공합니다.

Cisco ICFD는 노스바운드 API를 공개하여 고객이 하이브리드 클라우드 환경에서 워크로드를 프로그래밍 방식으로 관리하거나 선택한 관리 시스템과 통합함으로써 정책 및 거버넌스, 애플리케이션 설계 및 기타 기능을 포함하는 애플리케이션 관리를 보다 세부적으로 수행할 수 있도록 지원합니다. 이에 대해서는 이 문서의 뒷부분에서 살펴보겠습니다.

Cisco ICFD의 향후 릴리스에서는 Cisco Intercloud Fabric 솔루션을 차별화하는 향상된 서비스(예: 하이브리드 클라우드 환경에서 베어메탈 워크로드 구축)와 재해 복구 및 기타 서비스 구성 옵션을 지원하는 향상된 IT 관리 포털을 제공할 예정입니다.

셀프 서비스 IT 포털 및 서비스 카탈로그

Cisco ICFD 셀프 서비스 IT 포털에서는 IT 관리자가 하이브리드 클라우드 솔루션을 쉽게 관리 및 사용하고, 엔드 유저가 서비스를 쉽게 이용할 수 있습니다. Cisco ICFD는 여러 클라우드의 제품을 결합하는 서비스 카탈로그와 하이브리드 워크로드를 위한 단일 셀프 서비스 IT 포털을 엔드 유저에게 제공합니다.

Cisco ICFD에는 IT 관리자가 다음과 같은 관리 작업을 수행할 수 있는 IT 관리 포털이 있습니다.

- 퍼블릭 및 엔터프라이즈 프라이빗 클라우드에 대한 연결 구성
- 역할과 권한 및 엔터프라이즈 LDAP(Lightweight Directory Access Protocol) 통합 구성
- 테넌트 추가 및 관리
- 엔터프라이즈와 퍼블릭 클라우드 사이의 워크로드 배치를 규제하는 기본 비즈니스 정책 구성(관리 레이어에서 고급 정책 사용 가능)
- 포털 브랜드 맞춤화
- 용량 및 할당량 사용 모니터링
- 서비스 카탈로그를 검색하고 클라우드에서 워크로드 프로비저닝 및 관리 요청 시작
- 여러 클라우드의 워크로드를 보고 필요에 따라 워크로드 마이그레이션
- 사용자 정보 및 기본 설정 관리

- 카탈로그 및 이미지 자격 구성
- 가상 머신 템플릿 및 이미지 가져오기, 분류 및 자격 구성
- Cisco Intercloud Fabric Secure Extension 관리 수행
- 향후에 엔드 유저 또는 IT 관리 포털을 통해 기능을 추가할 수 있음

설치 용이성

Cisco ICFD는 고객이 몇 시간 이내에 초기 환경을 설정하고 서비스 사업자에 연결할 수 있는 간편한 설치 경험을 제공합니다. 또한 Cisco ICFD는 하이브리드 환경에서 워크로드 관리를 위한 단일 창으로서 Day 1 및 Day 2 운영을 개선하여 사업자 클라우드 액세스 구성과 환경 관리를 간소화해 줍니다.

Cisco Intercloud Fabric Secure Extension

모든 데이터 인 모션(data in motion)은 Cisco Intercloud Fabric Secure Extender 내에서 암호화된 상태로 격리됩니다. 이 데이터에는 프라이빗 및 퍼블릭 클라우드(Site-to-Site)와 클라우드에서 실행 중인 가상 머신(VM-to-VM) 간에 교환되는 트래픽이 포함됩니다. 이 데이터를 보다 안전하게 전송하기 위해 이러한 엔드포인트 사이에 DTLS(Datagram Transport Layer Security) 터널이 생성됩니다. DTLS는 UDP(User Datagram Protocol) 기반의 매우 안전한 전송 프로토콜입니다. Cisco Intercloud Fabric Extender는 항상 DTLS 터널 생성을 시작합니다.

사용되는 암호화 알고리즘을 구성할 수 있으며, 원하는 보안 레벨에 따라 다른 암호화 강도를 사용할 수 있습니다. 지원되는 암호화 알고리즘은 다음과 같습니다.

- AES-128-GCM
- AES-128-CBC
- AES-256-GCM(Suite B)
- AES-256-CBC
- 없음

지원되는 해싱 알고리즘은 다음과 같습니다.

- SHA-1
- SHA-256
- SHA-384

Cisco Intercloud Fabric Core Services

Cisco Intercloud Fabric에는 고객이 하이브리드 클라우드 환경에서 워크로드를 성공적으로 관리하는 데 필수적인 일련의 서비스가 포함되어 있습니다. 이 서비스는 Intercloud Fabric Core Services로 식별되며 다음과 같이 설명할 수 있습니다.

- **클라우드 보안** - Site-to-Site 및 VM-to-VM 통신의 보안 시행
- **네트워킹** - 스위칭, 라우팅 및 기타 고급 네트워크 기반 기능
- **VM 이식성** - VM 포맷 변환 및 모빌리티
- **관리 및 가시성** - 하이브리드 클라우드 모니터링 기능
- **자동화** - VM 라이프사이클 관리, 자동화된 운영 및 프로그래밍 방식 API

Cisco Intercloud Fabric의 향후 릴리스에서는 서드파티 어플라이언스 지원을 비롯한 확장된 일련의 서비스를 제공할 예정입니다.

Cisco Intercloud Fabric Firewall Services

기존 데이터 센터 구축에서는 가상화 시 가상 머신 간의 트래픽을 보호해야 하며, 이러한 트래픽을 일반적으로 동-서(east-west) 트래픽이라고 합니다. 조회를 위해 이 트래픽을 에지 방화벽으로 리디렉션하는 대신 데이터 센터에서 존 기반(zone-based) 방화벽을 구축하여 가상 환경에서 트래픽을 처리할 수 있습니다. Cisco Intercloud Fabric에는 구축 가능한 존 기반 방화벽이 포함되어 있어, 가상 머신 간 통신을 위한 정책을 시행하고 사업자 클라우드에서 동-서 트래픽을 보호할 수 있습니다. 가상 방화벽은 Cisco vPath(Virtual Path) 기술과 통합되어 지능형 트래픽 스티어링 및 서비스 체이닝을 지원할 수 있습니다. 존 기반 방화벽의 주요 기능은 다음과 같습니다.

- 네트워크 특성 또는 가상 머신 특성(예: 가상 머신 이름)을 기반으로 하는 정책 정의
- 존 기반(zone-based) 정책 정의: 정책 관리자가 매니지드 가상 머신 공간을 여러 개의 논리 영역으로 분할하고 논리 영역을 기반으로 방화벽 정책을 작성할 수 있습니다.
- 초기 플로우 조회 프로세스 후에 로컬 Cisco vPath 모듈에 대한 정책 결정을 캐싱하는 데 따른 성능 향상

Cisco Intercloud Fabric Routing Services

Cisco Intercloud Fabric Secure Extender는 엔터프라이즈 데이터 센터에서 사업자 클라우드에 이르기까지 레이어 2 확장을 제공합니다. 또한 트래픽을 엔터프라이즈 데이터 센터로 리디렉션하지 않고도 레이어 3 기능을 지원하기 위해 Cisco Intercloud Fabric에는 가상 라우터가 포함되어 있습니다. 가상 라우터는 검증된 Cisco IOS® XE Software를 기반으로 하며, 사업자 클라우드에서 가상 머신으로 실행됩니다. Intercloud Fabric에 의해 클라우드에 구축되는 라우터는 사업자 클라우드에서 실행 중인 워크로드에 대한 가상 라우터 및 방화벽 역할을 하며, 엔터프라이즈의 Cisco 라우터와 연동하여 엔드 투 엔드 Cisco 최적화 및 보안을 제공합니다. 가상 라우터에서 제공하는 주요 기능은 다음과 같습니다.

- 사업자 클라우드 내의 VLAN 간 라우팅
- 클라우드 가상 머신에 다이렉트 액세스
- 서비스 사업자의 데이터 센터에 대한 직접 VPN 터널을 통해 엔터프라이즈 지사에 연결
- 서비스 사업자가 지원하는 기본 서비스에 액세스(예: Amazon S3(Simple Storage Service) 또는 탄력적 로드 밸런싱 서비스 사용)

Cisco Secure Intercloud Fabric Shell

Cisco Secure ICF Shell(Secure Intercloud Fabric Shell)은 VM 그룹과 관련 클라우드 프로파일을 식별하는 하이 레벨 구조이며, 클라우드 간에 안전하게 이동 가능하도록 설계되었습니다. 클라우드 프로파일에는 다음과 같은 컨피그레이션이 포함됩니다.

- **워크로드 정책** - 확장할 네트워크, 클라우드에서 워크로드에 적용할 보안 시행, 기타 특성(예: DNS 컨피그레이션)을 정의하기 위해 엔터프라이즈 IT 관리자가 InterCloud Fabric Director 포털을 통해 작성하는 일련의 정책입니다.
- **Site-to-Site 및 VM-to-VM 보안 통신 정의** - IT 관리자는 프라이빗 클라우드와 퍼블릭 클라우드 간 및/또는 클라우드 내 VM 간의 보안 터널 구성을 관리, 활성화 또는 비활성화할 수 있습니다.

- **VM ID** - Intercloud Fabric은 관리하는 모든 VM에 대해 ID를 생성하여 신뢰할 수 있는 VM만 클라우드로 확장된 네트워크에 참여하거나, 퍼블릭 클라우드 내의 동일한 신뢰 범주 내의 다른 VM과 통신하거나, 프라이빗 클라우드 내의 다른 VM과 통신할 수 있도록 합니다.
- **클라우드 VM 액세스 제어** - Intercloud Fabric을 사용하면 프라이빗 클라우드와 퍼블릭 클라우드 간에 설정된 보안 터널을 사용하거나, Intercloud Fabric를 통해 정의 및 관리되는 VM 공용 IP를 사용하여 직접 클라우드 VM에 대한 액세스를 제어할 수 있습니다.

Cisco Intercloud Fabric for Providers

Cisco Intercloud Fabric for Providers는 사업자 클라우드 환경을 위한 것이며 엔터프라이즈 고객이 클라우드 환경 전반에서 동일한 수준의 보안 및 정책을 유지하면서 프라이빗 클라우드 환경을 사업자의 퍼블릭 클라우드로 투명하게 확장할 수 있도록 해줍니다. 사업자를 위한 두 가지 Cisco Intercloud Fabric 솔루션, 즉 매니지드 서비스를 제공하는 사업자를 위한 솔루션 또는 Intercloud Fabric 하이브리드 워크로드 대상인 사업자만을 위한 솔루션이 있습니다. 매니지드 서비스를 제공하려는 사업자를 위한 Cisco Intercloud Fabric for Providers는 다음과 같은 구성 요소로 이루어져 있습니다.

- Cisco Intercloud Fabric Director
- Cisco Intercloud Fabric Secure Fabric
- Cisco Intercloud Fabric Provider Platform

Intercloud Fabric 하이브리드 워크로드의 대상이 되고자 하는 사업자만을 위한 Cisco Intercloud Fabric for Providers는 다음과 같은 구성 요소로 이루어져 있습니다.

- Cisco Intercloud Fabric Provider Platform

Cisco Intercloud Fabric Provider Platform

Cisco ICFPP(Intercloud Fabric Provider Platform)는 다양한 퍼블릭 클라우드 API 작업과 관련한 복잡성을 간소화 및 추상화하고, 아직 클라우드 API 지원이 없는 서비스 사업자에 대한 클라우드 API 지원을 활성화합니다. Cisco ICFPP는 OpenStack, Cloudstack, VMware vCloud Director 및 Cisco에서 제공하는 SDK를 통해 통합될 수 있는 거의 모든 기타 API 등의 다양한 사업자 클라우드 인프라 관리 플랫폼과 통합될 수 있는 확장 가능한 어댑터 프레임워크를 제공합니다.

현재 서비스 사업자들은 독점 클라우드 API(Amazon EC2[Elastic Compute Cloud], Microsoft Windows Azure, VMware vCloud Director, OpenStack 등)를 사용하므로 고객이 다른 사업자로 전환하는 데 제약이 따르며 어려움이 있습니다. Cisco ICFPP는 이 복잡성을 추상화하고 Cisco Intercloud Fabric API 호출을 다른 사업자 인프라 플랫폼으로 변환하여, 고객이 서비스 사업자가 제공하는 클라우드 API에 상관없이 워크로드를 이동할 수 있도록 지원합니다.

많은 서비스 사업자가 Cisco Intercloud Fabric에서 고객 워크로드를 구축하는 데 사용할 수 있는 클라우드 API를 제공하지 못합니다. 이러한 사업자를 위한 한 가지 옵션으로 가상 머신 관리자의 SDK 및 API에 직접 액세스하는 방법이 있습니다(예: VMware vCenter 또는 Microsoft System Center를 통해 액세스). 이 경우 사업자 환경이 노출되므로 보안 문제가 있어 대부분의 경우 서비스 사업자에 적합한 옵션이 아닙니다. Cisco ICFPP는 사업자 클라우드 리소스를 사용하도록 허용하는 고객 클라우드에 대한 첫 번째 인증 지점으로, 사업자 환경에 매우 안전한 액세스를 구현하고 서비스 사업자가 Cisco Intercloud Fabric용 사업자 에코시스템에 참여하는 데 필요한 클라우드 API를 제공합니다.

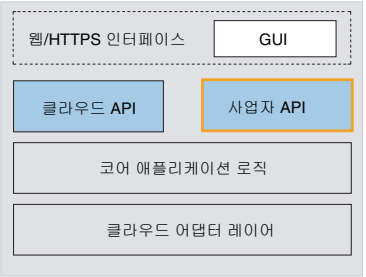
Cisco ICFPP는 고객 클라우드 환경의 Cisco Intercloud Fabric과 사업자 클라우드(퍼블릭 및 가상 프라이빗 클라우드) 사이에서 인터페이스 역할을 하며, 아래와 같은 다양한 이점을 제공합니다.

- 클라우드 API에 표준화 및 균일성을 적용하여 Cisco Intercloud Fabric에서 Cisco Intercloud Fabric 에코시스템에 포함된 서비스 사업자의 클라우드 서비스를 쉽게 사용할 수 있도록 지원
- 서비스 사업자의 기본 클라우드 플랫폼에 안전하게 액세스할 수 있도록 지원
- 고객 및 테넌트 환경별로 활용률을 제한
- 서비스 사업자가 기존 관리 플랫폼과 통합할 수 있도록 노스바운드(Northbound) API를 제공
- 멀티테넌시 지원
- 테넌트 레벨 리소스 모니터링 제공
- 향후에 Cisco 인프라별로 차별화 가능
- 향후에 엔터프라이즈에서 사업자 클라우드에 베어메탈 워크로드를 구축하도록 지원할 예정

Cisco ICFPP 아키텍처

Cisco ICFPP는 서비스 사업자 고객이 Cisco Intercloud Fabric API를 사용하여 클라우드 리소스에 액세스할 수 있도록 서비스 사업자의 클라우드 데이터 센터에 구축된 가상 어플라이언스입니다. 가상 어플라이언스는 고객의 Cisco Intercloud Fabric에서 공용 네트워크의 Cisco ICFPP 어플라이언스 인스턴스에 연결하고, Cisco ICFPP 어플라이언스에서 서비스 사업자 클라우드 플랫폼에 연결할 수 있도록 해주는 가상 네트워크 인터페이스를 제공합니다. 그림 2-2에서는 Cisco ICFPP 어플라이언스 아키텍처를 보여 줍니다.

그림 2-2 Cisco Intercloud Fabric Provider Platform 아키텍처



Cisco ICFPP 아키텍처는 다음과 같은 네 가지 주요 인터페이스 모듈로 구성되어 있습니다.

- **노스바운드 클라우드 API** - 이 모듈에서는 Cisco Intercloud Fabric(고객 클라우드)에서 워크로드를 프로비저닝하는 데 사용되는 Cisco Intercloud Fabric 클라우드 API를 구현합니다.
- **노스바운드 사업자 API** - 이 모듈에서는 서비스 사업자의 관리자가 Cisco ICFPP 어플라이언스를 구성하고, 테넌트 및 사용자를 프로비저닝하고, 테넌트 운영을 모니터링하는 데 사용하는 일련의 API를 구현합니다.
- **코어 애플리케이션 로직** - 이 모듈에서는 Cisco Intercloud Fabric 클라우드 API와 클라우드 플랫폼별 API 간 변환 로직을 구현합니다.
- **클라우드 어댑터 레이어** - 이 모듈에서는 OpenStack, CloudStack 또는 맞춤형 등과 같은 특정 클라우드 플랫폼과 연동하는 데 사용되는 다양한 클라우드 플랫폼 인터페이스 어댑터를 구현합니다.

Cisco ICFPP를 구축해야 하는 시기

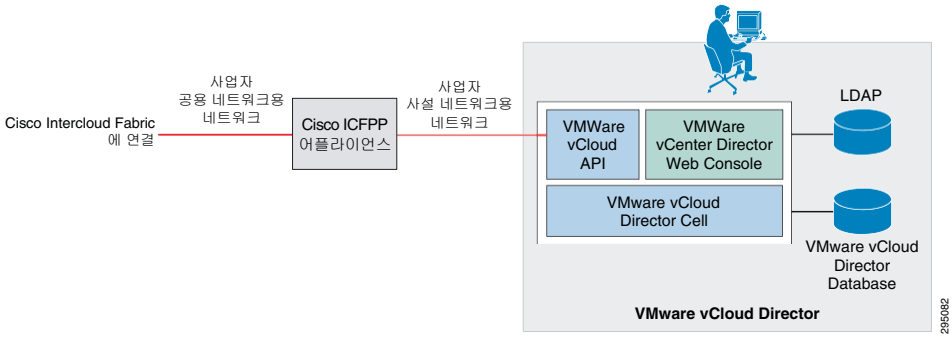
Cisco Intercloud Fabric과 연동되는 모든 서비스 사업자에 대해 Cisco ICFPP를 구현해야 합니다. 기본 퍼블릭 클라우드 API를 통해 Cisco Intercloud Fabric을 사용할 수 있는 Amazon EC2, Microsoft Windows Azure 및 IBM SoftLayer는 이 규칙의 유일한 예외 사항입니다.

Cisco ICFPP 구축 토폴로지

Cisco Intercloud Fabric에서 서비스 사업자의 클라우드 리소스에 액세스하려면 공용 네트워크에서 Cisco ICFPP 어플라이언스에 액세스해야 합니다. 따라서 서비스 사업자의 에지 라우터에 노출되는 사업자 네트워크에서 어플라이언스의 네트워크 인터페이스를 구축해야 합니다. 또한 네트워크 인터페이스에서 서비스 사업자 클라우드 플랫폼(예: OpenStack 또는 Cloudstack)에 액세스하는 프라이빗 사업자 네트워크에 연결해야 합니다.

Cisco ICFPP 구축 토폴로지는 서비스 사업자와 클라우드 플랫폼에 따라 다릅니다. 그림 2-3에서는 서비스 사업자의 VMware vCloud Director 환경을 통한 구축을 보여 줍니다.

그림 2-3 Cisco ICFPP 어플라이언스 구축 토폴로지



Cisco ICFPP 어플라이언스에서는 HTTPS 연결을 사용하여 Cisco Intercloud Fabric 및 서비스 사업자 클라우드 플랫폼과 통신합니다. Cisco Intercloud Fabric과 Cisco ICFPP 어플라이언스 사이 또는 Cisco ICFPP 어플라이언스와 클라우드 플랫폼 엔드포인트 사이의 네트워크 경로에는 방화벽이 필요하지 않지만, 방화벽을 사용하여 ICFPP와 주고받는 해당 트래픽 플로우만 강화할 수 있습니다.

Cisco ICFPP 운영 모델

다음 예에서는 Cisco ICFPP 어플라이언스에 Day 0 및 Day 1 운영에 대해 설명합니다.

Day 0 운영: 구축 및 초기화

Cisco ICFPP 어플라이언스는 서비스 사업자 데이터 센터에서 서비스 사업자 클라우드 플랫폼의 일부로 구축됩니다. Day 0 운영에서 서비스 사업자의 관리자는 사업자 네트워크에서 어플라이언스를 구축하고 다음과 같이 구성합니다.

- 어플라이언스 IP 주소
- 관리자 사용자 인증서 및 권한
- 클라우드 플랫폼 유형 및 엔드포인트 주소

서비스 사업자 관리자는 어플라이언스에 대한 서비스 사업자 테넌트 및 사용자를 프로비저닝합니다. Cisco ICFPP 어플라이언스를 구축한 후 서비스 사업자 관리자는 어플라이언스를 연결할 수 있도록 어플라이언스의 URL을 사업자의 고객에게 게시합니다.

Day 1 운영: 테넌트 사인온 및 쿼리

Cisco ICFPP 어플라이언스가 서비스 사업자 데이터 센터에서 작동하고 URL을 공개적으로 게시한 이후에는 사업자의 고객이 어플라이언스에 연결하고, Cisco Intercloud Fabric 구성 요소에서 사인온(sign-on) API 요청을 통해 Cisco ICFPP 어플라이언스에 액세스할 수 있습니다.

Cisco Intercloud Fabric 및 Cisco Validated Designs

VMDC(Virtualized Multiservice Data Center) Validated Design을 구축하는 Cisco Powered Cloud Providers 또는 대기업 고객을 위해 Intercloud Fabric은 특정 구성 또는 버전에 종속되지 않고 상호 보완됩니다. 클라우드 사업자의 경우 Cisco Intercloud Fabric for Provider와 선택한 클라우드 관리 플랫폼을 통합하고, 대기업 VMDC 고객의 경우 Intercloud Fabric for Business와 환경을 통합하여 VM Manager 및 선택한 클라우드 관리 플랫폼과 연동하고 필요한 경우 여러 클라우드 간에 워크로드를 이동 및 관리할 수 있습니다.

데이터 센터에서 FlexPod 또는 다른 Cisco Validated Designs을 구축하고 여러 클라우드 간에 워크로드를 안전하게 이동 및 관리하려는 고객의 경우, Intercloud Fabric for Business로 솔루션을 보완하고 이 문서의 앞부분에서 설명한 기능을 사용하여 가치를 증대할 수 있습니다. Intercloud Fabric for Business는 통합된 인프라의 VM Manager와 연동하며 하이브리드 클라우드 환경에서 워크로드를 관리하는 데 필요한 모든 리소스를 제공합니다.

Cisco Intercloud Fabric 및 관리 클라우드 플랫폼 통합

Cisco Intercloud Fabric에서 사설 리소스와 공용 리소스 사이에 구축된 원활한 보더리스 환경은 다양한 기능과 혜택을 제공합니다. 또한 클라우드 서비스, 애플리케이션 가시성 및 오케스트레이션, 애플리케이션 청사진 또는 구축 프로파일 등에 대한 자동 배치 결정 혜택을 제공하기 위해 기업에서는 노스바운드 API를 통해 Cisco Intercloud Fabric과 통합되는 선택형 관리 클라우드 플랫폼을 사용할 수 있습니다.

관리 클라우드 플랫폼은 사용 가능한 노스바운드 REST(Representational State Transfer) API를 통해 Cisco ICFD에 연결되어, ICFD 리소스에 대한 작업을 수행하고 업스트림 포털 및 오케스트레이션 시스템과 통합될 수 있습니다. 현재 ICFD는 다음과 같은 API 작업을 지원합니다.

- 정책 관리
- VDC 관리
- 카탈로그 작업
- 과금 관리
- 워크플로 관리
- 감사 관리
- 가상 머신 작업

다른 API 작업은 제품의 향후 릴리스에 추가될 예정입니다. Cisco ICFD REST API는 HTTP 및 HTTPS 프로토콜과 호환되며 JSON 및 XML 서식 코드를 지원합니다. Java API도 사용할 수 있습니다. API 문서는 cisco.com/go/intercloudfabric에서 확인해 주십시오.

결론

Cisco Intercloud Fabric은 하이브리드 클라우드를 채택할 때 가장 일반적으로 발생하는 대부분의 과제를 해결합니다. 또한 하이브리드 클라우드를 사용하는 엔터프라이즈 고객에게 필수적인 보더리스 환경을 구축하고, 서비스 사업자가 엔터프라이즈 고객이 사용할 퍼블릭 클라우드 제품을 제공할 수 있도록 해줍니다.

또한, Cisco Intercloud Fabric을 사용하면 유연성과 엔터프라이즈급 보안이 내장되고 비즈니스 요구 사항을 미러링하는 워크로드 정책을 작성할 수 있습니다. Cisco Intercloud Fabric에서는 이러한 클라우드 전반의 워크로드를 확인할 수 있는 단일 창을 제공하고 다양한 하이퍼바이저 및 클라우드 사업자 리소스를 지원하여 멀티 클라우드 환경에 일관된 정책 및 보안을 제공할 수 있습니다. 또한, Cisco Intercloud Fabric은 비인가 섀도우 IT 구축을 보기로 가져와서 IT 이해관계자가 애플리케이션을 해당 환경에 안전하게 구축할 수 있도록 도와줍니다.

이 솔루션은 기본적으로 제공되고 API에서 지원하므로 유연하게 구현되며 광범위하고 독립적인 통합을 보장합니다.

부록 A

섀도우 IT 및 Cisco Cloud Consumption Professional Services

Cisco Cloud Usage Collector를 고객 네트워크에 구축하면 비인가 클라우드 애플리케이션, 즉 섀도우 IT를 식별할 수 있습니다. NetFlow 데이터를 고객 라우터에서 컬렉터로 전송하여 액세스 중인 클라우드 서비스 사업자, 사용중인 고유 IP 주소 수, 해당 사업자에 대한 트래픽 볼륨 등을 식별합니다. 이 정보는 섀도우 IT 소비를 보여 줍니다.

클라우드 컴퓨팅은 IT 환경을 획기적으로 변화시켰습니다. 비용을 절감하고 비즈니스 민첩성을 강화하기 위해 기업은 온프레미스 위주의 IT 구조에서 클라우드와 온프레미스 애플리케이션이 혼합된 구조로 변화하고 있습니다. 2014년에는 IT 예산의 약 10%가 클라우드 서비스에 지출되고, 2020년까지 클라우드 시장이 1,590억 달러 규모로 성장할 것으로 예상됩니다.

퍼블릭 클라우드 서비스 도입이 증가하면서 비인가 클라우드 애플리케이션도 증가하고 있습니다. 이러한 섀도우 IT는 기업에서 회사의 IT 인프라에 통합되거나 이를 통해 관리되지 않는 퍼블릭 클라우드를 구현할 때 발생합니다. 대부분의 IT 팀에서는 자사에 섀도우 IT가 존재한다는 사실을 알고 있지만, 회사에 접속하는 클라우드 애플리케이션의 수는 알지 못합니다. 고객과 함께 실시한 초기 평가에 따르면 승인된 클라우드 서비스 벤더의 경우 일반적으로 실제 클라우드의 20%만 사용하지만, 사용되고 있는 클라우드 서비스의 수는 IT 팀에서 파악하고 있는 것보다 5~10배 더 많습니다.

이러한 트렌드는 업계 설문조사에서도 나타납니다. 자문 회사인 CEB에서 최근에 실시한 설문조사에 따르면, 165개 조직의 CIO(Chief Information Officer)들은 섀도우 IT가 공식 IT 예산의 40% 이상(470억 달러 이상의 IT 지출)을 차지할 것으로 예상합니다. 또한 Gartner는 IT 부서에서 IT 예산을 통제할 수 없게 될 것으로 예상합니다. 2015년에는 대부분의 기업에서 엔터프라이즈 IT 지출 중 35%가 IT 부서의 예산과는 별도로 관리될 것입니다(2012년 이후 IT 조직 및 사용자에 대한 Gartner 주요 예측).

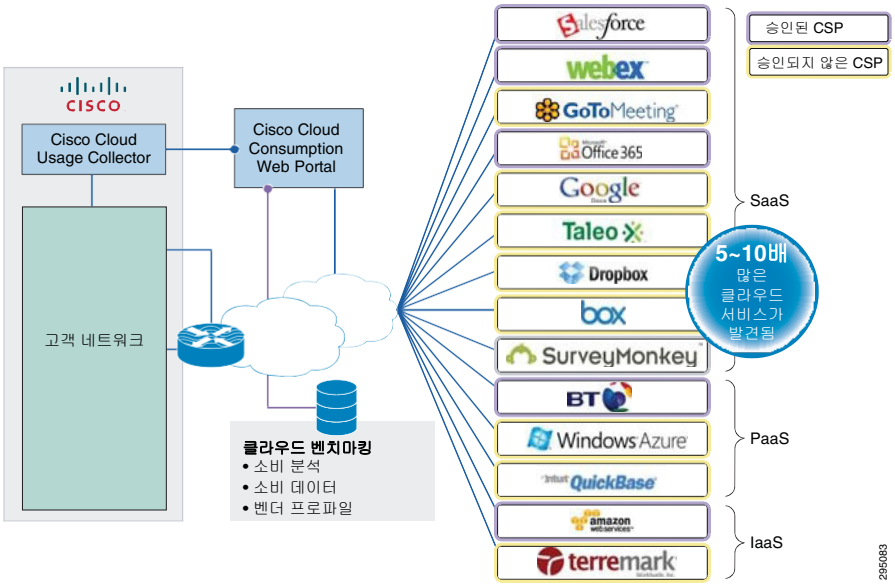
섀도우 IT는 비즈니스와 IT 리더들에게 클라우드 도입 관련 비용과 위험을 관리하는 방법, 클라우드 관리 프로세스를 효과적으로 설정하는 방법 등의 새로운 과제를 제시합니다.

Cisco Cloud Consumption Professional Services는 고객이 클라우드 서비스를 파악하고 강력한 클라우드 관리 방식을 구현하도록 돕기 위해 제작되었습니다. Cisco Cloud Consumption Professional Services는 고객이 더욱 민첩하게 대처하고, 위험을 줄이고, 퍼블릭 클라우드 비용을 최적화하도록 도와줍니다. Cisco Cloud Consumption Professional Services에서는 네트워크를 사용하여 고객이 조직 전체에서 직원들이 액세스 중인 CSP(Cloud Service Provider)를 확인할 수 있도록 도와줍니다. 고객은 이 서비스를 통해 조직에서 승인된 퍼블릭 클라우드 사용과 무단 사용을 정확하게 파악할 수 있습니다.

고객 네트워크에 데이터 수집 툴을 배치하면 Cisco에서 조직 전반의 클라우드 서비스 사업자 이용 데이터를 수집하여 중복 클라우드 서비스, 퍼블릭 클라우드 지출, 잠재적 위험, 클라우드 사용 추세 등을 식별할 수 있습니다.

Cisco Cloud Consumption Professional Services에서는 일반적으로 IT 부서에서 승인한 것보다 5~10배 더 많은 클라우드 서비스를 검색하고 조직에 클라우드 사용 관련 위험 및 비용을 파악할 수 있는 툴을 제공합니다(그림 A-1).

그림 A-1 섀도우 IT 제어



예를 들어, 캐나다 뉴브런즈윅 정부의 IT 부서에서는 공용 인터넷 트래픽의 90%를 차단하고 11개의 클라우드 사업자만 승인했음에도 불구하고 Cisco Cloud Consumption Assessment Service를 통해 220개 이상의 클라우드 사업자를 적발했습니다. 이는 750,000달러의 잠재적 비용절감이 가능한 수준입니다.

Cisco Cloud Consumption Professional Services는 Cisco Advanced Services를 통해 Cisco Intercloud Fabric 솔루션에 애드온으로 제공되지만, 향후 릴리스에서는 이 기능을 제품에 완전히 통합할 예정입니다.