

VMware vShield Edge

데이터 센터의 에지 네트워크 보안

요약 정보

VMware vShield 가상화 보안 제품군 중 하나인 VMware vShield™ Edge는 가상 데이터 센터를 위한 포괄적인 네트워크 경계 보안을 제공합니다. vShield Edge는 VMware vSphere®과 매끄럽게 통합되며 클라우드 인프라를 신속하고 안전하게 확장하도록 지원하는 필수 네트워크 게이트웨이 서비스를 제공합니다.

주요 장점

- 네트워크 게이트웨이 서비스를 신속하게 프로비저닝하므로 특수 용도의 여러 어플라이언스를 사용할 필요가 없어 비용과 복잡성 감소
- 기본 제공된 에지 네트워크 보안 및 서비스로 정책 적용 보장
- 조직 또는 테넌트당 1개의 에지로 확장성과 성능 증대
- 상세 로깅을 통해 IT 규정 준수를 간편하게 수행
- VMware vCenter™ Server 및 업계 선두의 엔터프라이즈 보안 솔루션과 통합된, 모든 기능을 완벽히 갖춘 인터페이스를 사용하여 관리 작업 간소화

vShield Edge 개요

vShield Edge는 가상 데이터 센터용 에지 네트워크 보안 솔루션으로, 네트워크 보안 게이트웨이 서비스 및 웹 로드 밸런싱과 같은 필수적인 보안 기능을 제공하여 성능과 가용성을 보장합니다. 이 솔루션은 vSphere로 직접 연결할 수 있으며 탁월한 유연성을 제공하기 위해 Fault Tolerance, 고가용성 등의 기본 제공 기능을 활용합니다.

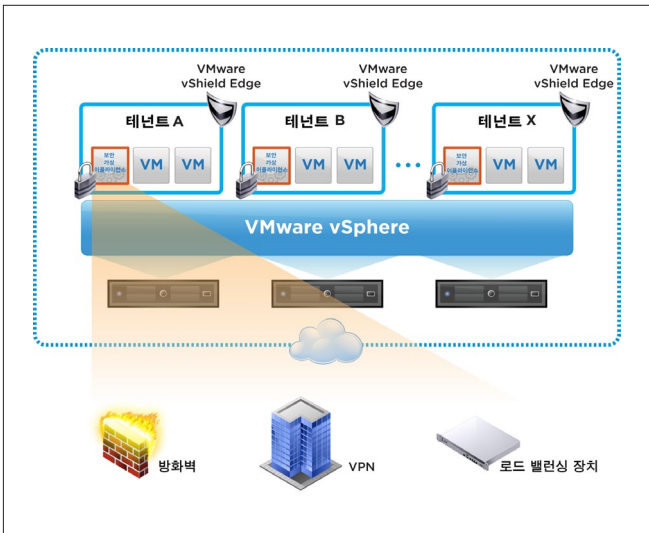
관리자는 vCenter Server에 매끄럽게 통합되어 가상 데이터 센터의 보안 관리 통합을 촉진하는 vShield Manager 콘솔을 통해 중앙에서 vShield Edge를 관리할 수 있습니다. 또한 vShield Edge는 VMware vCloud™ Director와 연동되어 멀티 테넌트 클라우드 인프라 내의 가상 데이터 센터에 대한 안전한 프로비저닝을 자동화 및 가속화합니다. 동시에, 보안 및 가상 인프라 관리자의 업무를 구분하여 인증된 리소스에게만 액세스를 허용합니다.

vShield Edge의 작동 방식

가상 어플라이언스로 구축되는 vShield Edge는 방화벽, 웹 로드 밸런싱 장치, NAT(네트워크 주소 변환) 및 DHCP 서비스를 제공하여 소스 및 대상 IP 주소에 대한 패킷 헤더를 모니터링합니다. 또한 정책에 따라 연결을 거부 또는 허용하고, VPN 세션을 실행 또는 종료하며, 네트워크 주소 변환을 수행하고, 소스 또는 대상 포트와 프로토콜 유형(TCP 또는 UDP)별로 데이터를 검사할 수 있습니다.

vShield Edge의 기능

- **에지 보안 하드웨어 통합** – vShield Edge는 기존의 vSphere 리소스를 사용하여 에지 보안 서비스를 프로비저닝하기 때문에 vSphere 호스트 간에 “에어 갭”을 적용하기 위한 에지 보안 하드웨어가 필요하지 않습니다.
- **가상 데이터 센터 경계를 신속하고 안전하게 프로비저닝** – vShield Edge를 통해 하드웨어에 독립적인 보안 논리적 경계 (“에지”)를 가상 데이터 센터 환경 주위로 간단하게 생성하므로 멀티 테넌트 IT 인프라 내의 공유 네트워크 리소스를 더욱 쉽게 활용할 수 있습니다.
- **공유 네트워크상의 데이터에 대한 완벽한 보안 유지** – vShield Edge는 256비트 암호화와 함께 사이트 간 VPN을 제공하여 여러 가상 데이터 센터 사이에서 전송되는 모든 데이터의 보안을 완벽하게 유지합니다.
- **웹 서비스의 성능과 가용성 보장** – vShield Edge는 가상 머신 클러스터 전체에 발생하는 인바운드 웹 트래픽을 효과적으로 관리하고 고객이 에지 보안과 함께 또는 별도로 구축할 수 있는 웹 트래픽 로드 밸런싱 기능을 제공합니다.



vShield Edge는 기본 제공되는 경계 보호 기능으로 가상 데이터 센터 간의 트래픽을 보호합니다.

- **규정 준수 관리 지원** – vShield Edge는 상세 이벤트 로깅, 플로우 통계 등 업계 및 정부 규정과 기업 정책에 대한 준수 사실을 입증하기 위해 기업이 필요로 하는 필수 제어 기능을 제공합니다.

주요 특징

방화벽

- NAT(네트워크 주소 변환)가 필요 없는 경계(계층 3) 방화벽
- 다음을 기준으로 인바운드/아웃바운드 연결 제어 규칙을 사용하는 상태 추적 방화벽
 - IP 주소 – 소스/대상 IP 주소
 - 포트 – 소스/대상 포트
 - 프로토콜 – 유형(TCP 또는 UDP)

NAT(네트워크 주소 변환)

- 가상화된 환경 내외부로 IP 주소 변환
- 신뢰할 수 없는 위치에 대해 가상 데이터 센터 IP 주소를 마스크 레이딩

DHCP(Dynamic Host Configuration Protocol)

- vSphere 환경 내의 가상 머신으로 자동 IP 주소 프로비저닝
- 관리자 정의 매개 변수(예: 주소 풀, 리스 기간, 전용 IP 주소)

사이트 간 VPN

- 가상 데이터 센터(또는 에지 보안 가상 머신) 간 안전한 커뮤니케이션
- IKE(Internet Key Exchange) 프로토콜에 기반하여, 공유 키와 인증서 인증을 지원하는 IPsec VPN

웹 로드 밸런싱

- 웹 트래픽(HTTP)을 비롯한 모든 트래픽에 대한 인바운드 로드 밸런싱
- 라운드 로빈 알고리즘
- 세션 라우팅(sticky session)

에지 플로우 통계

- 가상 데이터 센터 리소스 활용도를 측정하고 테넌트로 다시 귀속시킵니다.
- 통계가 REST(Representational State Transfer) API를 통해 액세스되고 서비스 공급업체 차지백 애플리케이션에서 활용됩니다.

정책 관리

- vShield Manager를 통해 완전한 기능으로 관리 수행(상당수의 기능이 vCenter Server 인터페이스를 통해서도 액세스 가능)
- REST API를 사용하는 맞춤형 관리용 인터페이스
- 엔터프라이즈 IT 보안 관리 툴 지원

로깅 및 감사

- 업계 표준 syslog 형식 기반
- REST API 및 vShield Manager 사용자 인터페이스를 통해 액세스 가능
- 주요 에지 보안 이벤트(오류, 경고 등)에 대한 관리자 정의 로깅 설정/해제
 - 방화벽: 규칙 수준에서 실행
 - NAT: 규칙 수준에서 실행
 - VPN: 사이트 간 연결 이름
 - 웹 로드 밸런싱 장치: 풀 수준에서, URL 또는 풀더를 포함한 웹 요청에 따라 실행
 - DHCP: 서비스 수준, 바인딩(릴리스와 갱신)에 따라 실행

지원되는 릴리스

vSphere 환경에 지원되는 릴리스에 대한 자세한 내용은 <http://www.vmware.com/products>를 참조하십시오.

관련 제품

이 밖에도 vShield 제품군에는 네트워크 기반 공격으로부터 애플리케이션을 보호하고 민감한 데이터를 검색하는 VMware vShield App with Data Security, VMware 엔드포인트 보안과 가상 데이터 센터의 성능을 강화하는 vShield Endpoint, vShield Manager 그리고 이 모든 제품이 포함된 vShield Bundle이 있습니다.

추가 정보

자세한 정보를 찾거나 VMware 제품을 구입하려면 1-877-4-VMWARE(한국 지사 (02) 6001-3890)로 전화하거나 <http://www.vmware.com/products>를 방문하거나 인증된 재판매자를 온라인으로 검색하십시오. 제품 규격 및 시스템 요구 사항에 대한 자세한 내용은 VMware vShield 관리 가이드 (http://www.vmware.com/pdf/vshield_41_admin.pdf)를 참조하십시오.

vShield 제품에 대한 자세한 내용은 <http://www.vmware.com/products>에서 확인하십시오.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMware, Inc. 서울시 강남구 삼성동 159-1번지 아셈타워 37층 (우) 135-798 전화: (02) 6001-3890 e-메일: korea-sales@vmware.com

Copyright © 2011 VMware, Inc. All rights reserved. 본 제품은 미국 및 국제 저작권 및 지적 재산권 법률의 보호를 받습니다. VMware 제품은 여러 건의 특허 보호 대상이며 일부는 특허 출원 중입니다. 자세한 내용은 웹 사이트(<http://www.vmware.com/go/patents>)를 참조하시기 바랍니다. VMware는 미국 및/또는 기타 관할 지역에서 VMware, Inc.의 등록 상표 또는 상표입니다. 이 문서에 언급된 기타 명칭과 표시는 모두 해당 소유권자의 상표입니다. Item No: VMW-DS-vSHLD-EDGE-A4-102_KR