White Paper

Array SSL VPN 전용 솔루션

Fast, Secure and Scalable Secure Access

AG 시리즈 Secure Access Gateway

목차

개요

기업은 원격 액세스 요구를 해결하기 위해 수년에 걸쳐 SSL (Secure Sockets Layer) 기반의 가상 사설망 (VPN)으로 전환해 왔습니다. 개인과 기업 소유 스마트 모바일 장치의 확산에 따라 기업의 데이터와 중요 자원에 대한 안전한 모바일 액세스의 필요성이 다시 강조되었습니다. 업계 분석가들에 따르면:

스마트 폰의 대중화와 인터넷에 연결된 스마트 폰, 태블릿, 넷북 그리고 기타 모바일 장치의 확산으로 각 기업들은 본사, 지사, 원격 사무실 및 데이터 센터의 중요 인프라가 악성코드로부터 어떻게 보호되고 있는지 재평가하고 있습니다 - "Infonetics Research1"

엔터프라이즈의 변화하는 특성과 엔터프라이즈 네트워크에 연결되는 모바일 장치의 증가는"Consumerization of Enterprise"로 인해 조직이 네트워크 보안에 대한 새로운 접근 방식이 요구되고 있습니다.- "ABI Research2

일반적으로 본인의 랩톱을 사용하는 계약직과 게스트와 같은 외부 인원의 경우 각 디바이스의 보안 상태가 매우 다양하고, 내부 사용자들 또한 점점 더 이동성과 특성이 다양해지고 있기 때문에 기업과 서비스 프로바이더들은 최종 사용자에게 제공하는 응용 프로그램과 네트워크 리소스에 대한 안전한 액세스를 필수적인 환경으로 만들려고 합니다.

일반적으로 SSL VPN 은 사용자가 여러 장소와 컴퓨팅 장치로부터 안전하게 데이터와 응용 프로그램에 액세스 할 수 있게 하고 세분화 된 사용자 인증 기반의 접근 제어를 제공합니다. 그러나 최근에는 SSL VPN 이 방화벽이나 차세대 방화벽에 추가되는 기능으로 점점 더 많이 등장하게 되었습니다. 시스템자원에 대한 의존성이 높은 다른 보안 어플라이언스에 SSL 처리는 통합하는 경우 대규모 사용자가 요구하는 확장성에 대한 제약과 최종 사용자 경험에 필요한 성능에 부정적인 영향을 줄 수 있습니다.

방화벽/SSL VPN 통합 솔루션의 문제점

SSL VPN 솔루션은 브라우저에서 사용되는 것과 동일한 SSL 프로토콜을 사용하여 트래픽을 암호화하여 데이터의 기밀성과 무결성을 제공합니다. 일반적으로 SSL VPN 을 IPsec 또는 전용 회선 VPN 을 기반으로 하는 원격 액세스 방법에 비해 나은 원격 액세스 솔루션으로 인식되고 있습니다.

그러나 많은 SSL VPN 공급 업체들은 거의 클라이언트리스와 클라이언트/서버 응용 프로그램에 대한 액세스 제어를 제공 할 때 SSL VPN 의 유연성과 보안성에만 초점을 두었습니다. 따라서 SSL VPN 솔루션의 전반적인 확장성과 성능에 대한 고객의 요구 사항과는 상당한 차이가 있었습니다.

1 http://www.businesswire.com/news/home/20120308006173/en/Infonetics-Research-Network-Security-Market-Set-Stronger

2 https://www.abiresearch.com/market-research/product/1006059-world-enterprise-network-and-data-security/

또한 많은 SSL VPN 솔루션들이 방화벽이나 차세대 방화벽에 하나의 모듈 또는 옵션으로 제공되고 있어 다음과 같은 영역에서 기업 고객의 요구를 충족시키기에는 불충분 했습니다.

- **성능과 사용자 경험** –대기 시간과 처리 성능 요구 사항을 충족시키고 최종 사용자 경험을 향상시켜 최종 사용자의 생산성 향상이 가능할 것
- **확장성** – 단일 하드웨어 플랫폼에서 성능의 저하 없이 다수의 동시 사용자를 지원할 수 있게 확장할 수 있는 능력
- **보안** – 전체 시스템의 성능을 떨어뜨리지 않으면서 암호화, 심층 패킷 검사 그리고 응용 프로그램 레벨의 필터링 제공

성능

몇 년 전부터 사이버 보안 업계는 이전의 1024 비트 표준보다 훨씬 안전하지만 CPU 소모가 5 배 가량 많은 2048 비트 암호화로 전환하였습니다. SSL VPN 을 방화벽이나 차세대 방화벽과 같은 컴퓨팅 작업이 많은 다른 제품에 통합하면 SSL VPN 의 성능에 영향을 미치는 컴퓨팅 자원을 놓고 경합이 생겨 결과적으로는 사용자 경험과 작업자 생산성이 저하될 수 있습니다.

예를 들어, SSL 대량 암호화를 생각해 보겠습니다. 대부분의 add-on SSL VPN 솔루션은 SSL Key 교환시에는 SSL VPN co-processor 하드웨어를 사용합니다. 하지만, data 와 같은 대량 암호화는 메인 CPU 를 사용합니다. 대량 암호화는 CPU 처리량이 많은 작업이기 때문에 시스템 처리량에 큰 타격을 주며 특히 2048 비트 키를 사용하면 상당한 지연이 발생합니다.

응용 프로그램 관점의 처리량은 또 다른 중요한 요소입니다. SSL VPN 은 대부분의 통합 플랫폼에서는 감당하기 어려운 정도의 부하를 처리하도록 요구하고 있습니다. 따라서 이에 대한 적절한 설계가 이루어지지 못한 통합 SSL VPN 플랫폼은 금방 지원 가능한 사용자 수의 한계에 부딪히게 됩니다. 지원되는 동시 사용자 수나 처리량 또는 두 가지 측면 모두가 공급 업체가 명시한 한계치 보다 실제로는 훨씬 낮을 수 있습니다. 결과적으로 이들은 제대로 작동하지 않거나 기능이 제대로 작동하지 않아 최종 사용자의 생산성을 저해합니다.

고객은 요구되는 성능 기준을 달성하기 위해 여러 대의 통합 SSL VPN 장비를 구입하는 경우가 발생하고, 처리량과 동시 사용자 지원 측면에서 요구 성능보다 훨씬 낮은 수준으로 작동해야 하는 상황을 맞을 수가 있습니다. 물론 이는 초기 투자 비용과 지속적인 관리 비용을 증가시키고 장애 지점(point of failure)이 늘어남에 따른 신뢰성 하락을 가져 옵니다.

일부 조직에서는 성능 저하로 인해 별도의 타사 응용 프로그램 가속 솔루션을 구입하여 운영하기도 합니다. 이는 다시 비용 상승과 신뢰성 저하로 이어집니다.

확장성

이러한 비용을 피하려면 확장성이 뛰어난 SSL VPN 솔루션을 찾는 것입니다. 확장성이란 주로 최대 동시 사용자 수와 최대 동시 SSL 커넥션 수의 두 가지 요소로 측정됩니다. 또한 더 많은 보안 계층, 규칙, 다양한 커뮤니티를 위한 가상 포털 등을 갖춘 매우 복잡한 SSL VPN 구성은 확장성에 영향을 줄 수 있습니다.

Add-on SSL VPN 솔루션은 동시 사용자를 최대 25,000 명까지 확장 할 수 있다고 주장 할 수 있지만, 위에서 언급 한 것처럼 실제 지원 가능한 규모는 훨씬 적습니다. 그러나 25,000 명의 동시 사용자 수 조차도 많은 대규모 기업 및 서비스 제공 업체한테는 너무 적은 규모 입니다.

SSL VPN 관리 서비스를 제공하는 서비스 제공 업체의 경우 단일 시스템에서 25,000 명 이상의 사용자와 수백 명의 고객으로 확장 할 수 있는 능력이 필수적입니다. 대부분의 글로벌 2000 기업이 10 만 명 이상의 직원을 고용하고 있다는 사실을 감안할 때 많은 대기업에서도 마찬가지입니다.

모든 직원이 안전한 원격 액세스를 필요로 하는 것은 아니고 모든 사람이 동시에 로그인하는 것은 아니지만 SSL VPN 을 직원만

사용하는 것은 아닙니다. 많은 경우 계약직, 파트너, 공급 업체 그리고 필요한 경우 고객에게도 보안 액세스 권한을 부여해야 합니다. 단순하고 클라이언트가 없는 특성을 감안할 때 대부분의 IT 전문가는 이러한 다양한 그룹 및 개인의 보안 액세스 요구 사항을 충족시키기 위해 SSL VPN 을 사용하는 것을 선호합니다. 그러나 SSL VPN 솔루션이 시스템 당 사용자의 일반적인 한계를 초과하여 확장 될 수 없다면 구조적으로나 경제적으로 그러한 까다로운 요구 사항에 부합할 수 없습니다.

또한 비즈니스 단위, 파트너 또는 고객의 그룹에 따라 서로 다른 수준의 액세스 권한을 갖기를 원합니다. 물론 방화벽/SSL VPN 통합 솔루션도 다양한 사용자 그룹에 대해 세부적인 역할 기반 정책을 지원할 수 있지만 각 그룹별 사용자 포털을 보호하기 위해 별도의 어플라이언스가 필요할 수 있습니다. 결과적으로 다양한 사용자 집단이 추가 될 때 총 소유 비용 (TCO)이 급등 할 수 있습니다.

보안

따라서 방화벽/SSL VPN 통합 플랫폼의 성능과 확장성 측면의 단점은 보안 기능 자체를 제한하는 데 중요한 역할을 하기도 합니다. 왜냐하면, 적절한 수준의 보안을 제공하려면 시스템의 처리 능력이 필요합니다. 통합 SSL VPN 솔루션에서는 사용자가 50 명 정도 밖에 없을 때는 원하는 수준의 보안을 설정할 수 있지만 사용자가 추가되면 성능이 저하됩니다. 따라서 IT 관리자는 원하는 성능이 나오지 않으면 보안 수준을 낮춰서 성능을 맞추려는 유혹을 받을 수 있습니다. 분명히 이것은 문제가 있는 전략입니다.

통합 SSL VPN 의 또 다른 문제점은 OpenSSL 과 같은 상용 또는 오픈 소스 운영 체제 일 수 있기 때문에 해당 운영 체제와 관련된 모든 취약점과 보안 허점을 함께 가지게 됩니다. 대부분의 통합 SSL VPN 에는 고급 보안 기능이 결여되어 있어 이러한 기능을 위해 다른 보안 장치를 추가하여야 하는 경우가 많고, 이로 인한 시스템 구성상의 복잡성과 비용의 증가와 함께 지연시간이 늘어날 수 있습니다. 또한 방화벽/SSL VPN 통합 솔루션은 일반적으로 클라이언트와 SSL VPN 장비 구간의 보안을 제공할 뿐 어플라이언스- 서버간의 보안을 담당하지는 않습니다. 이로 인해 사용자는 모든 보안 위협의 상당 부분을 차지하는 내부 공격에 취약해지게 됩니다. (IBM 의 2016 Cyber Security Intelligence Index 에 따르면 모든 공격의 60 %는 내부자의 부주의 또는 악의적인 공격으로 인한 것입니다.)

전용 SSL VPN

앞서 살펴본 방화벽/SSL VPN 통합 솔루션과 관련된 여러 가지 단점은 전용 SSL VPN 솔루션이 해결할 수 있습니다. 이 전용 어플라이언스는 Array Networks 가 제공하는 고성능 AG 시리즈 SSL VPN 장비를 제공하는 것과 같은 접근 방식입니다.

Array Network AG 시리즈 전용 어플라이언스는 ArrayOS ™ 운영 체제를 실행하는 전용 플랫폼을 기반으로 하며, 방화벽/SSL VPN 통합 플랫폼과 비교하여 능률적인 운영으로 대규모 동시사용자 지원과 SSL 세션 처리 그리고 고성능 처리 및 낮은 대기 시간이 특징입니다.

다목적 통합 컴퓨팅 플랫폼에서는 여러 기능의 처리를 위해 여러 계층의 처리 과정을 거쳐야 하기 때문에 상당한 병목 현상과 대기 시간을 초래합니다. 이에 반해 ArrayOS 운영 체제는 처리를 간소화하고 CPU 집약적인 작업이 하드웨어에서 수행되도록 최적화 하였습니다.

[3] http://www-03.ibm.com/security/data-breach/cyber-security-index.html

SSL VPN 아키텍처 비교

고려 사항	SSL VPN/Firewall 통합형	Array 전용 SSL VPN
2048-bit SSL 및 Bulk 암호화 처리를 위해 강력한 프로세싱 파워 요구	CPU 자원을 방화벽과 공유해야 함	고성능의 SSL VPN 전용 CPU
사용자 증가에 대한 대응	동시 사용자 수에 제한이 있고, 사용자 증가 시 하드웨어 추가가 필요할 수 있음.	단일 어플라이언스에서 최대 13 만 명의 동시 사용자 지원. 오버 헤드 관리 및 TCO 절감
강력한 암호화 처리 및 적정 성능 유지 필요함	방화벽과 리소스를 공유하기 때문에 성능 보장을 위해 보안 수준을 낮춰야 할 수 있음.	전용 CPU 로 성능 저하 없이 고도의 맞춤화 된 보안 제공
오픈 소스 또는 일반적인 상용 OS 는 고급 보안 기능이 부족하고 취약점에 노출 될 수 있음	고급 보안을 위해 추가 하드웨어가 필요할 수 있고 서버가 위험에 처할 수 있음.	강력한 보안과 높은 성능을 위해 특별히 설계된 맞춤형 운영 체제 및 하드웨어

탁월한 성능과 사용자 경험

실제로 Array SSL VPN 전용 플랫폼은 경쟁 제품(통합형 또는 전용어플라이언스형)에 비해 최대 8 배의 빠른 성능, 처리량 및 용량을 제공 할 수 있습니다. 이러한 성능과 처리 능력이 가능한 것은 대부분 ArrayOS 및 SpeedStack®라는 독자적인 처리 엔진 때문입니다. 이 엔진은 여러 기능을 처리함에 있어서 TCP 오버헤드가 발생하는 여러 번의 데이터 플로우 없이 한번의 데이터 이동만으로 처리하도록 해 줍니다. 아래 그림의 통합된 여러 features 들의 처리시 데이터를 이동하지 않고 메모리의 데이터를 직접 액세스하는 것을 보여주고 있습니다.

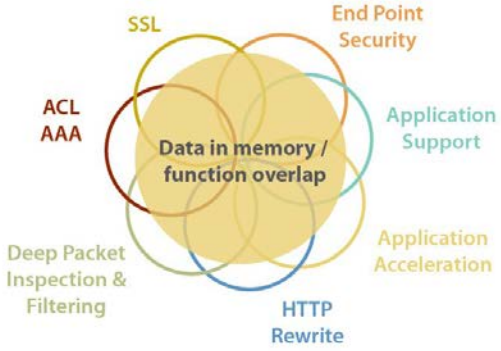
여러 functions 들이 여려 features 들로 구성되어 있다는 것을 생각해보면 많은 features 들의 중첩이 발생합니다. 이는 어느 한 시점에 하나의 function 이 호출되면 한 개 이상의 features 가 서비스 되기 때문에 자원의 효율적인 활용과 성능의 향상이 가능해 집니다.

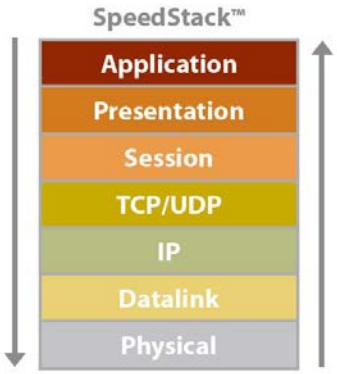
Array SSL VPN 은 SSL 키 교환과 대량 암호화 처리를 하드웨어에서 수행하는 것 외에도, 압축과 커넥션 다중화 기능을 통합하여 응답 시간을 향상시키고 네트워크 연결 작업의 부하를 줄여 서버의 작업 부하를 줄여 줍니다. 결과적으로 500 명의 동시 SSL 사용자가 평균 웹 페이지 응답 시간은 2ms 에 불과하기 때문에 수천 명의 동시 사용자 지원에도 응답시간을 한자리 수 이내로 유지합니다.

응용 프로그램 서버의 비용 때문에 고성능의 TCP 네트워크 작업을 수행하기 어렵고 원격 사용자에 대한 WAN bandwidth 확장도 어려운 환경을 지원하기 위해 Array AG 시리즈는 업계 최고의 TCP 커넥션 다중화, 하드웨어 기반 HTTP 압축과 같은 여러 가지 응용 프로그램 가속 기능을 동시에 제공합니다. 이러한 높은 수준의 기능과 성능으로 서버 응답 시간을 단축하고 최종 사용자 경험을 향상시키면서 비용을 절감합니다.

사용자 경험의 품질 관점에서 보면, 고성능 SSL VPN 솔루션이 없는 경우 LAN 속도에 익숙한 사무실 근로자는 WAN 을 통해 원격으로 접속시 아마도 좌절하고 포기할 수 있을 것입니다. 또한 VPN 솔루션에 대한 경험이 부족한 근로자의 경우 불가피하게 발생할 수 밖에 없는 로그인과 사용법 등에 관해 교육이 필요하기도 할 것입니다. Array AG 시리즈는 이 두 가지 문제를 완화시켜 줄 수 있습니다.

[4] See Appendix A for performance testing results on all AG Series models.





강화된 보안

Array SSL VPN 전용 플랫폼의 강력한 성능은 성능을 유지시키기 위해 보안 수준을 낮추는 일이 없다는 것을 의미 합니다. 실제로 방화벽/SSL VPN 통합 솔루션에서는 성능을 유지시키기 위해 보안 수준을 낮추는 일들이 발생하기도 합니다.

다른 SSL VPN 솔루션과 마찬가지로 Array 솔루션도 인증, 권한 부여 및 감사 (AAA) 그리고 Cache cleaning 을 포함한 엔드 포인트 보안을 지원합니다. 이뿐만 아니라 Array SSL VPN 은 일반적인 방화벽/SSL VPN 통합 솔루션에서는 제공하지 않는 수많은 보안 기능을 내장하고 있습니다.

보안이 강력한 이유는 ArrayOS 운영체제가 독자적인 운영체제라는 데서 출발합니다. Windows 나 Linux 와 같은 범용 OS 에 포함되어 있는 SSL VPN 운영에 불필요한 기능과 그 기능에 수반되어 발생하는 보안 취약점이 전혀 없습니다. ArrayOS 는 보안이 강화된 운영체제로 잠재적 공격 영역을 줄입니다. 또한, Array AG Series 는 독자적인 SSL Stack 을 사용하고 있기 때문에 대부분의 타 SSL VPN 벤더들이 사용하는 OpenSSL 이 안고 있는 많은 취약점들에 대해 자유로운 SSL VPN 솔루션입니다.

ArrayOS 는 완전한 리버스 프록시 아키텍처를 사용합니다. 즉, 백엔드 서버와의 연결 전에 클라이언트와의 모든 연결을 종료한 뒤 서버와 새로운 연결을 설정합니다. 여기에는 여러 가지 목적이 있습니다. 첫 번째는 외부의 공격으로부터 백엔드 서버를 보호하는 것입니다. 모든 연결이 어레이 SSL VPN 에서 일단 종료되기 때문에 클라이언트 측 장치에서는 백엔드 서버를 직접 볼 수 없습니다. 또한 Array 는 응용 프로그램에 연결하기 전에 커넥션을 완전히 종료한 뒤 다시 연결하는 delayed connection 기법을 사용합니다. 이렇게 하면 스푸핑 된 IP 주소가 올바르게 종료되지 않기 때문에 스푸핑 된 IP 주소가 서버에 연결되는 것을 막습니다.

Array AG 시리즈는 wire-speed stateful 방화벽과 L7 패킷 검사를 적용하여 비정상적인 패킷을 즉시 감지하고 삭제합니다. 특히 엔드-투-엔드 보안이 요구되는 중요한 애플리케이션에 대해서는 Array AG 시리즈와 백엔드 서버 간의 세션도 다시 암호화 할 수 있습니다.

확장성 있고 가상화 된 범용 액세스 솔루션

앞서 설명한 바와 같이 대기업과 서비스 프로바이더는 다양한 사용자를 지원할 수 있도록 최고의 확장성, 최저의 TCO 그리고 유연한 액세스 제어를 요구 합니다. Array AG Series 는 업계 최고의 확장성, 가상화 그리고 액세스 제어 기능을 통해 이러한 엄격한 요구 사항을 충족합니다.

한 대의 시스템으로 지원할 수 있는 최대 값:

- 130,000 concurrent users
- 3 Gbps throughput
- 256 virtual portals.

256 개의 가상 포털은 각각 고유 한 액세스 정책과 보안 구성 및 화면 디자인 등을 따로 구성할 수 있습니다. 즉, 직원이 e-mail, ERP 및 CRM 등에 액세스 하기 위한 직원용 포털, 파트너를 위한 포털, 고객사를 위한 포털들 다양한 형태의 독립적인 포털을 운영할 수 있습니다. 또한 서비스 제공 업체의 경우 단일 시스템에서 최대 256 명의 고객사를 지원할 수 있기 때문에 타 SSL VPN 솔루션과 비교하여 프로비저닝 및 운영 비용을 대폭 절감 할 수 있습니다.

액세스 제어와 관련하여 ArraySSL VPN 솔루션은 범용 SSL VPN 과 비교하여 비약적인 발전을 이루었습니다. Array SSL VPN 은 여러 LAN 스위치, SSL VPN 장비 및 별도의 무선 LAN 스위치에서 ACL 을 설정하고 유지 관리 할 필요가 없습니다. Array 의 SSL VPN 을 사용하면 사용자가 회사에서 제공한 장비 또는 개인 소유의 장비에서 원격지 또는 무선 랜에서 네트워크에 액세스 하든지 간에 각기 적합한 접근 통제 방법을 제공합니다.

보안 액세스는 Array SSL VPN 의 다음과 같은 핵심적인 특징의 수에 따라 결정됩니다.

- 가장 많은 동시 사용자 및 세션 수 지원과 함께 낮은 응답 시간 및 높은 처리량으로 생산성을 저하시키지 않으면 서 많은 수의 사용자를 지원합니다.
- 조직에서 현재 운영중인 방화벽 ACL 을 대체 할 수 있는 고성능 네트워크 및 응용 프로그램 방화벽을 통합했습니다.
- 다양한 사용자 그룹에 대해 최대 256 개의 가상 포털을 제공하므로 원격지이든 스마트 모바일 장치를 통해 네트워크에 액세스하든 관계없이 많은 수의 사용자를 위해 여러 포털을 쉽게 지원하고 관리 할 수 있습니다.
- 보안 및 네트워크 정책 관리 책임을 IT 부서의 적절한 담당자에게 위임 할 수 있는 고급 role-based 관리 기능을 제공합니다.

Array 는 사용자의 엔드포인트에 대한 보안을 한 곳 즉, Array SSL VPN 에서 정의할 수 있도록 합니다. 따라서 여러 LAN 스위치, 방화벽, SSL VPN 장비 및 별도의 WLAN 스위치등에서 ACL 을 정의하지 않아도 됩니다.

요구사항 충족

AG 시리즈가 확장 가능한 액세스, 향상된 보안 및 우수한 성능을 결합하여 제공함에 따라 고객은 비용과 시간을 크게 절약 할 수 있습니다. 단일 시스템으로 모든 원격 액세스 요구 사항을 충족 할 수 있기 때문에 여러 대의 방화벽/SSL VPN 통합 시스템을 사용하는 것과 비교할 때 TCO 가 크게 낮아집니다. 또한 Array 가 제공하는 고급 보안 기능과 액세스 요구 사항을 중앙에서 제어 할 수 있기 때문에 비용 절감 효과는 더욱 커집니다. 동시에 Array 는 고객에게 향후 VPN 에 대한 추가적인 요구 사항을 지원할 수 있는 토대를 제공합니다.

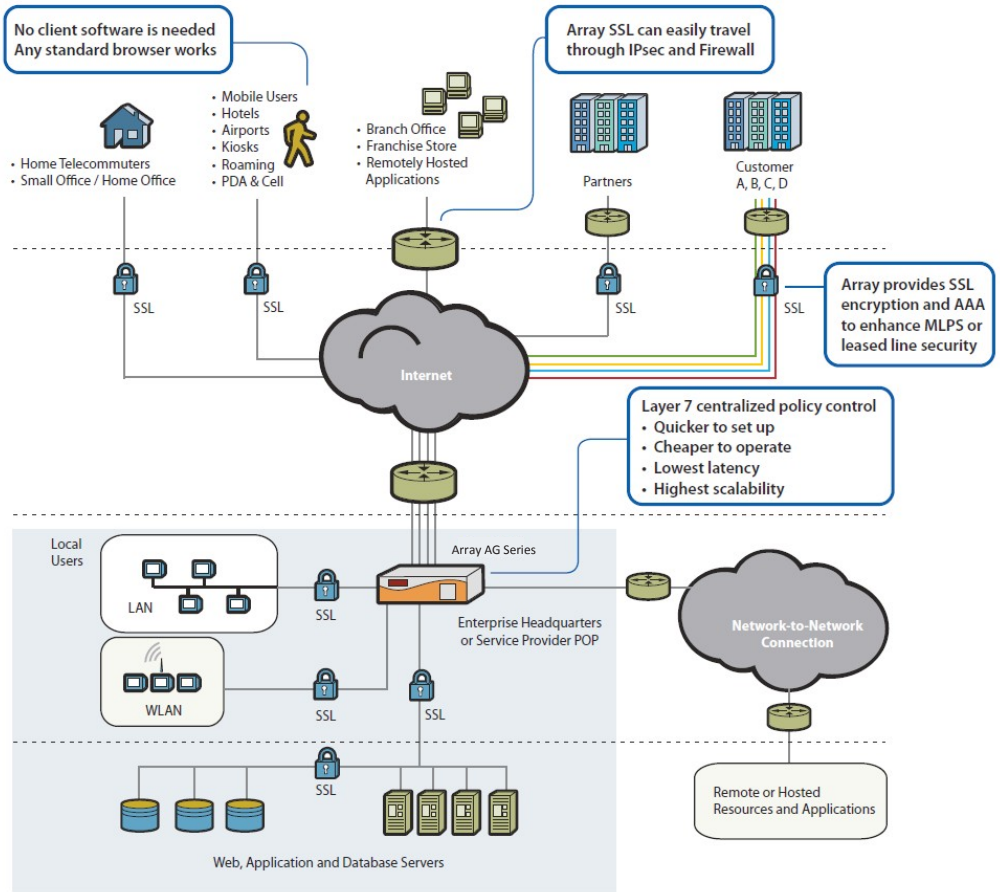
높은 성능, 낮은 TCO

Array 의 시스템당 최대 동시 사용자 수는 130,000 명으로 사용자 당 비용을 고려할 때 매우 낮은 TCO 를 제공합니다. AG 시리즈는 1,000 명 이하의 사용자일 경우에도 비용 효율성이 높지만, 높은 사용자 수에서는 비용이 더욱 큰 폭으로 감소합니다. 이에 반해 경쟁 솔루션의 경우 사용자가 1,000 명이 넘어가면 더 많은 어플라이언스를 추가해야 하고 이로 인한 관리의 복잡성이 증가 하기 때문에 TCO 가 더욱 높아집니다. 또한 Array 의 멀티플렉싱 기술 덕분에 백엔드 서버의 부하는 줄어 들어 결과적으로 서버 하드웨어와 소프트웨어 비용이 줄어들어 TCO 가 더욱 낮아집니다.

예를 들어, 130 억 달러 규모의 헬스케어 회사에서 2 개월 이내에 5,000 명을 네트워크에 접속시키는 솔루션을 찾기 위하여 VPN 과 씬 클라이언트가 고려되었습니다. 검토 결과 Array SSL VPN 솔루션이 선정되었는데 그 이유는 경쟁 솔루션에 비해 훨씬 높은 성능과 안정성 그리고 보안성을 제공했기 때문이었습니다.

Array 시스템은 사용자당 단지 $40 의 비용이 드는 반면, 경쟁 솔루션의 경우 $200 이상이 소요되었습니다. 또한 헬프 데스크의 부담이 훨씬 적고 관리가 간편하여 경쟁 솔루션과 비교했을 때 Array 시스템의 총 비용 절감액이 1 백만 달러 이상이었습니다.

다른 헬스케어 회사인 Presbyterian Healthcare 도 의사 및 기타 직원이 환자 정보에 안전하게 접속할 수 있도록 Array SSL VPN 을 도입했습니다.



이전 솔루션에 비하여 최종 사용자의 응답 시간이 50% 향상 되었고 동시에 처리 할 수 있는 동시 사용자 수가 100% 증가했습니다. 또한 Microsoft IIS 웹 서버가 기존에 약 800 명을 처리했던데 반해 서버 당 약 4,000 명의 사용자를 처리할 수 있게 되어 서버 처리능력이 최대 400 % 증가한 것을 볼 수 있습니다. 결과적으로 이 조직은 필요한 백엔드 서버 수를 50% 줄였습니다.

마찬가지로 1 억 명 이상의 고객에게 이동 통신 서비스를 제공하는 세계 최대의 통신 서비스 제공 업체 중 한 곳은 헬프 데스크 직원 운영에 연간 310 만 달러를 지출하여 이 서비스 업체의 기업 고객들에게 IPsec 기반 VPN 액세스 솔루션을 관리 할 수 있도록 지원하고 있습니다. 이 솔루션이 2,000 명의 동시 사용자를 초과하여 확장 할 수 없었지만 공급 업체는 이미 5,000 개의 공급 업체 커뮤니티를 보유하고 있으며 계속 성장하고 있었습니다. Array Networks 의 SSL VPN 으로 전환하여 클라이언트측 지원과 교육이 더 이상 필요하지 않기 때문에 헬프데스크 비용을 대폭 절감 할 수 있었습니다. 또한 Array 시스템은 회사 규모가 큰 5 천 개의 공급 업체를 쉽게 지원할 수 있게 되었고, 고객은 충분한 확장 여력도 가지게 되었습니다.

Array 의 가상화 기능은 방화벽/SSL VPN 통합 솔루션에 비해 상당한 비용 절감 효과를 가져옵니다. 각 그룹에 대해 별도의 SSL VPN 장비를 구입하고 관리하는 것과 달리 하나의 플랫폼에서 모든 다양한 사용자 그룹 (직원, 파트너, 공급 업체 및 고객)을 지원할 때의 비용 절감 효과를 생각해보십시오. AG 시리즈를 사용하는 서비스 제공 업체는 단일 플랫폼으로 최대 256 개의 고객을 지원할 수 있을 뿐 아니라 더 이상 고객사에 어플라이언스를 설치 할 필요가 없기 때문에 초기 비용과 지속적인 관리 비용을 크게 절감 할 수 있습니다.

Array 시스템을 사용하면 이제 고객은 더 이상 성능을 유지하기 위해 보안을 희생해야 하는 걱정을 할 필요가 없습니다. AG 시리즈는 특수목적의 아키텍처를 기반으로 하고 있고 CPU 집약적인 작업은 하드웨어서 처리하도록 구현되어 있기 때문에 경쟁 솔루션을 훨씬 능가하는 성능을 제공할 수 있습니다. 또한 통합 웹 방화벽 기술을 제공하기 때문에 이러한 기능을 처리하기 위해 추가 보안 제품을 구입할 필요가 없으므로 TCO 가 추가로 절감됩니다.

유비쿼터스 보안 : 액세스 제어

TCO 의 또 다른 측면은 조직에서 사용자 액세스 정책을 처리하는 방식과 관련이 있습니다. 이 프로세스는 종종 비효율, 중복 및 복잡성으로 가득합니다. 대부분의 조직에서는 동일한 사용자에 대해 네트워크 내의 수많은 지점에서 다음과 같은 사용자 액세스 정책을 정의해야 합니다.

- SSL VPN : 원격 사용자 액세스 제어
- WLAN 스위치:무선 액세스 제어
- LAN 스위치 : 유선 액세스 제어
- Firewalls
- Proxy 서버 : 이메일 및 여러 애플리케이션 서버를 위한 프록시

이러한 방식으로 여러 번 정책을 정의하는 것은 관리 비용이 많이 들 뿐만 아니라 모든 정책이 동기화되어 있는지 확인하기가 어렵기 때문에 의도하지 않은 보안 취약점이 발생됩니다.

Array SSL VPN 솔루션을 이용하면 IT 관리자는 한 곳에서 최종 사용자의 액세스 정책을 정의 할 수 있으므로 여러 스위치 및 어플라이언스에서 ACL 을 설정하고 유지 관리 할 필요가 없습니다.

사용자가 기업 보안 정책을 준수하는 경우도 있고 그렇지 않은 경우도 있을 수 있는 수 많은 종류의 장치를 이용하여 언제 어디에서든 회사 네트워크에 로그온 할 수 있는 유비쿼터스 환경이 되어감에 따라 액세스 제어가 매우 중요합니다.

기업의 임직원, 비즈니스 파트너 또는 게스트가 인터넷 서핑이나 원격으로 작업 중에 자신도 모르게 자신의 디바이스가 악성코드에 감염될 수 있고 이러한 장치들이 기업의 네트워크에 직접 연결될 수 있습니다.

이러한 종류의 위험들은 어떤 조직에서도 있어서는 안 되는 상황입니다. 특히, 기업의 데이터 및 고객 개인정보 보호와 같이 엄격한 규제 준수를 해야 하는 경우에는 더욱 그렇습니다.

기업은 사용자의 신원, 장치 및 네트워크 사용 권한의 모든 측면을 하나로 묶은 중앙 집중식 접근 제어 솔루션이 필요하며 제어하지 않는 그룹에 대해서도 정책을 동일하게 적용 할 수 있습니다.

Array 솔루션은 다음과 같은 보안 기능을 제공합니다. :

- 클라이언트측 보안 점검을 통해 클라이언트 컴퓨터가 회사 보안 정책을 준수하는지 점검합니다. 액세스 제한, 공격시 패치서버로의 리다이렉션, 특정 응용 프로그램이나 환경에 대한 액세스 제한 등 여러 가지 방어수단을 사용할 수 있습니다.
- 인트라넷 및 엑스트라넷에 대한 역할 기반 보안 액세스, 웹 응용 프로그램 보호를 위한 URL 마스킹을 통해 웹 응용 프로그램에 안전하게 액세스 할 수 있습니다.
- 파일서버 및 클라이언트/서버 애플리케이션에 대한 안전한 액세스를 제공합니다.
- 각 그룹별로 관리 권한을 적합한 IT 담당자에게 위임할 수 있는 역할기반의 관리가 가능합니다.
- 내장 된 일회용 암호 인증, 타 벤더의 다중 인증 지원 그리고 MS AD, RADIUS 또는 Array 장비 자체의 인증 데이터베이스와의 결합을 통한 강력한 인증이 가능합니다.
- 네트워크 및 애플리케이션 레벨의 통합 방화벽을 포함하고 있습니다.

Array AG 시리즈는 많은 수의 동시 사용자 및 세션을 지원할 수 있고, 높은 처리량과 짧은 응답 시간 때문에 대규모 환경에서 보안 액세스를 처리하는 데 적합한 유일한 플랫폼 입니다.

씬 클라이언트 애플리케이션에 대한 보안

Array AG Series 는 웹 응용 프로그램, 전자 메일, 파일 서버 등에 안전하게 액세스 할 수 있을 뿐만 아니라 Citrix 및 Windows Terminal Server 를 비롯한 씬 클라이언트 응용 프로그램에 중요한 보안 계층을 제공합니다.

예를 들어, Array SSL VPN 시스템을 Citrix 서버 앞에 배치하면 조직의 네트워크 노출이 줄어 듭니다. 원격 클라이언트는 일반적으로 회사 네트워크에 설치된 Citrix 서버에 직접 연결됩니다. 즉, Citrix 서버에 대한 액세스 권한을 얻은 침입자도 마찬가지로 나머지 네트워크에 액세스 할 수 있습니다.

Array 의 리버스프록시 아키텍처는 이러한 위협을 제거합니다. 모든 원격 세션은 Array 시스템에서 종료되며 Array 시스템이 Citrix 서버와의 연결을 다시 설정하여 원격 사용자가 다른 네트워크 리소스에 액세스하지 못하게 합니다. Citrix 서버는 Array AG 시리즈로 보호되는 하나의 응용 프로그램이 됩니다.

Array AG 시리즈는 또한 관리자가 사용자 액세스 권한을 URL, 디렉토리 또는 응용 프로그램 수준까지 세밀하게 제어 할 수 있게 해줍니다. 또한 Array 는 로그인 할 때부터 로그 아웃 할 때까지 모든 사용자 작업을 포괄하는 향상된 감사 기능을 제공합니다.

리얼타임 트랜잭션을 위한 솔루션

많은 기업들이 응답 시간에 대한 보다 엄격한 요구 사항에 직면 해 있습니다. 웹 사이트에서 더 나은 성능을 요구하는 고객뿐만 아니라 ERP 시스템에 액세스하는 외부 사용자도 응답이 나올 때 까지 마냥 기다리는 것을 원치 않을 것입니다..

시간은 곧 돈입니다. 예를 들어, 금융 서비스 분야에서는 대용량의 자금 거래는 적절한 시간에 액세스하고 거래가 이루어져야 하기 때문에 빠른 응답 시간이 필수적입니다. 주식 가격은 문자 그대로 매 초 매 분 단위로 변동됩니다. 문제는 많은 주식 거래자들이 사무실에 있는 것이 아니기 때문에 문제가 복잡해집니다. 설사 그들이 고객을 방문하는 길에 있을 때에도 안전하고 빠르게 주식거래 애플리케이션에 접속할 수 있어야 합니다.

이 경우 SSL VPN 솔루션이 좋은 선택이 될 수 있습니다. 이는 각 클라이언트 컴퓨터에 IPsec 소프트웨어를 설치하고 유지 관리하는 것보다 훨씬 간단하기 때문입니다. 그러나 방화벽/SSL VPN 통합 솔루션은 대규모 사용자 환경에서 필요로 하는 응답 시간 (일반적으로 5ms 미만)을 제공하기에 충분하지 않습니다.

사이트-사이트 VPN

SSL VPN 이 원격 액세스 부문에서는 IPsec VPN 을 분명히 대체했지만 사이트 간 VPN 연결에는 여전히 IPSec 이 널리 사용됩니다. 단일 시스템에 연결되는 사용자의 수가 사이트 간 구성에서 훨씬 많기 때문에 시스템의 확장성이 높아야 합니다. Array AG Series 는 사이트 간 VPN 연결을 지원하는 허브-스포크 SSL VPN 터널링 솔루션인 Site2Site 를 지원하며, 최대 130,000 명의 동시 사용자와 256 개의 가상 포털을 지원할 수 있는 Array 는 SSL VPN 이 분야에서도 경쟁력을 가질 수 있게 되었습니다.

요약

SSL VPN 기술은 2008 년 Gartner 가 "SSL VPN" 이 주요 업무에 대한 원격 액세스 방법으로 채택될 것이라고 예측한 이후 원격 액세스 방법에서 IPSec 과의 경쟁에서 승자가 되었습니다. 그러나 SSL VPN 사용이 증가하고 모바일 장치가 등장하면서 액세스, 보안 및 성능에 대한 요구 또한 증가 했습니다..

방화벽/VPN 통합 솔루션은 성능, 확장성, 보안성, 최종 사용자 경험 및 다양한 방식의 액세스를 제공하는 기능면에서 요구 사항을 충족시키기에는 전용 SSL VPN 에 비해서는 부족한 점이 많습니다.

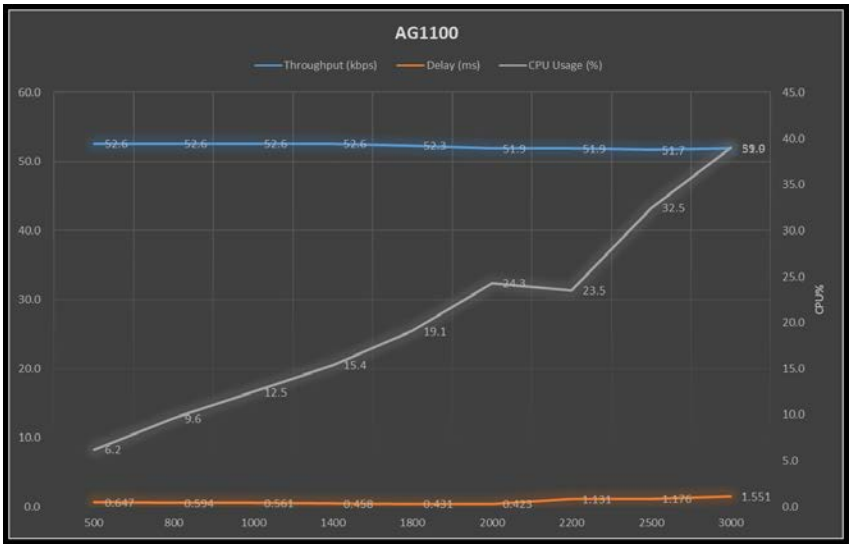
SSL VPN 요구 사항을 철저하게 충족시킬 수 있도록 설계된 전용 플랫폼 만이 대기업과 서비스 프로바이더의 요구를 충족시킬 수 있습니다. Array AG 시리즈 보안 액세스 게이트웨이는 독자적인 ArrayOS 운영 체제와 함께 가장 까다로운 요구 사항을 충족시킬 수 있는 능력을 가지고 있으며 최대 13 만 명의 동시 사용자를 지원합니다. 또한 256 개의 포털 지원은 다른 벤더에서는 대적할 데가 없습니다.

이러한 기능은 오늘날의 SSL VPN 에 대한 다양한 요구 사항을 충족할 수 있을 뿐만 아니라 미래의 VPN 요구 사항까지 충족할 수 있는 유일한 플랫폼으로 확장할 수 있습니다.

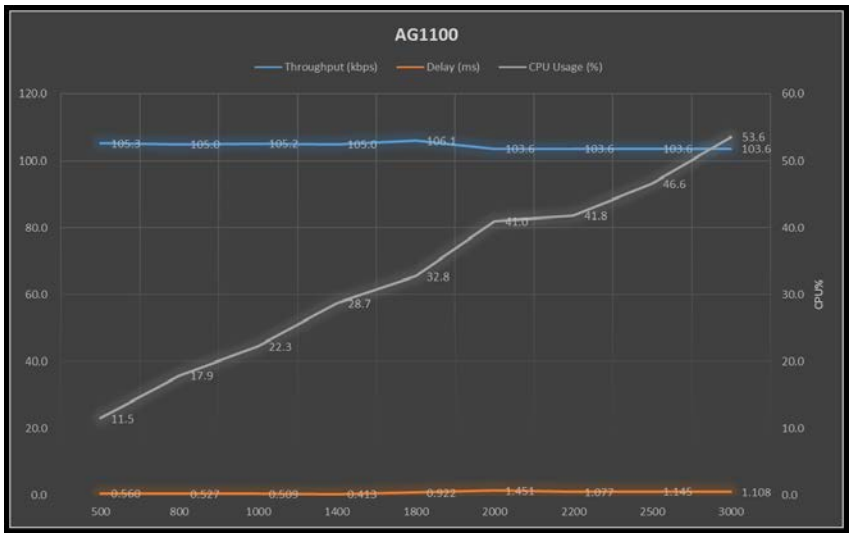
Appendix A

자체 테스트를 통해 어레이 AG 시리즈 SSL VPN 장비의 강력한 성능과 처리량을 입증 할 수 있습니다. 다음은 일련의 AG 시리즈 모델에 대한 그래픽 테스트 결과입니다.

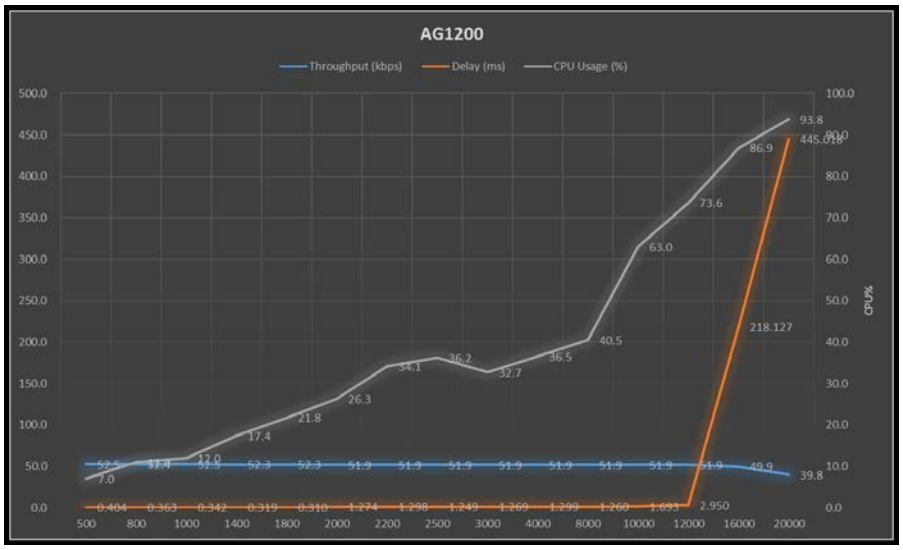
AG1100 : 50kbps throughput/user :



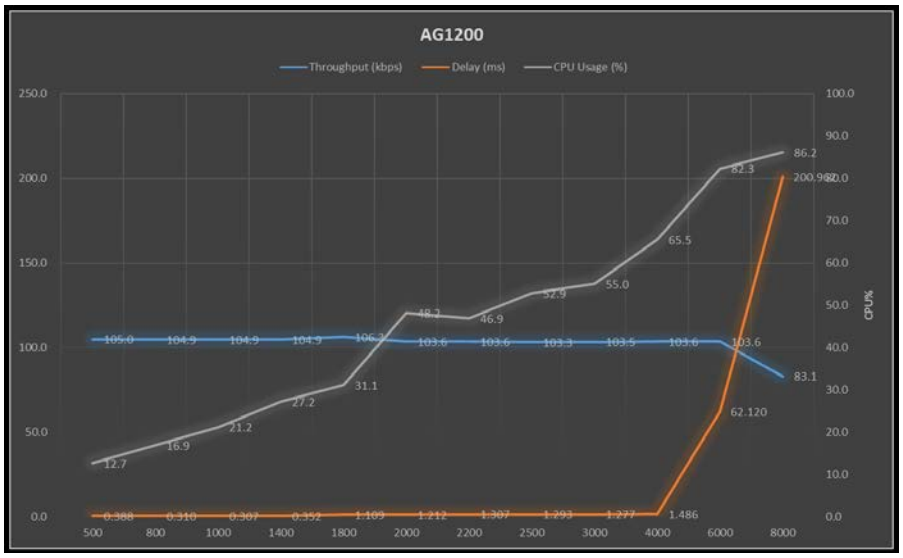
AG1100 : 100kbps throughput/user :



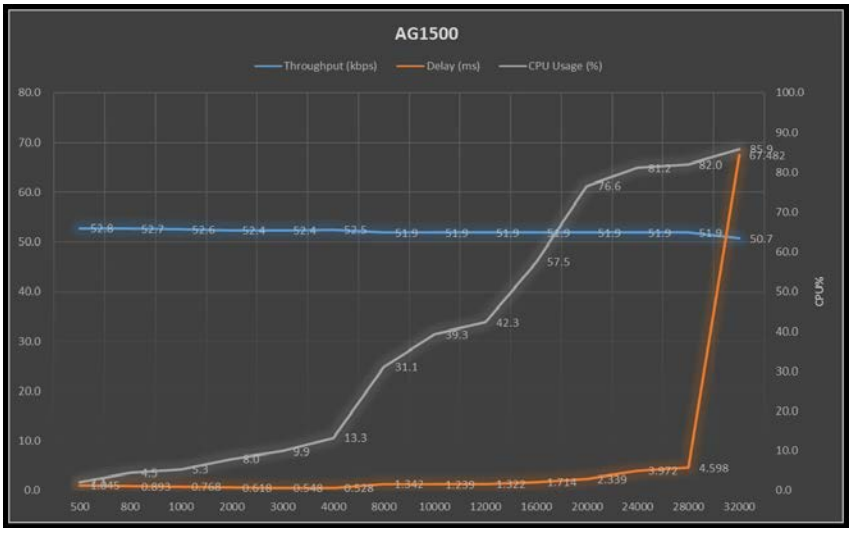
AG1200 : 50kbps throughput/user :



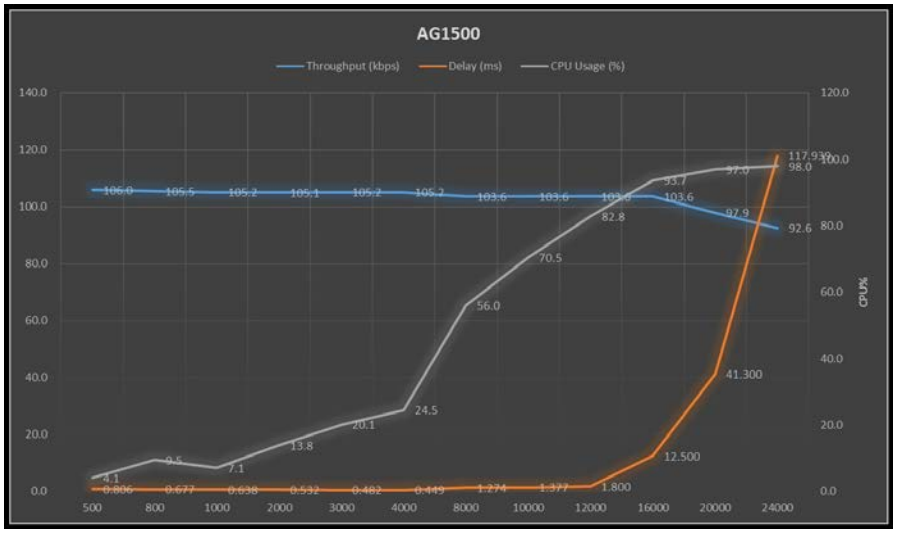
AG1200 : 100kbps throughput/user :



AG1500 : 50kbps throughput / user:



AG1500 : 100kbps throughput/user:



About Array Networks

Array Networks 는 전세계적으로 5,000 개 이상의 고객을 둔 애플리케이션 딜리버리 네트워킹 분야의 글로벌 리더입니다. 수상 경력이 있는 SpeedCore® 소프트웨어를 기반으로 하는 APV(어레이 애플리케이션 딜리버리), WAN 최적화 및 보안 액세스 솔루션은 최고의 엔터프라이즈, 서비스 제공 업체 및 공공 부문으로부터 탁월한 성능과 총 소유 가치를 인정 받고 있습니다. Array 는 실리콘 밸리에 본사가 있으며 전 세계 250 명이 넘는 직원이 지원하고 있으며 강력한 투자자, 관리 및 매출 성장을 이룬 수익성 있는 회사입니다. Deloitte, IDC 및 Frost & Sullivan 으로부터 기술 혁신, 운영 효율성 및 시장의 기회에 잘 준비된 기업으로 인정 받았습니다.

문의처 :

www.arraynetwork.co.kr
array-sales@arraynetwork.co.kr

Feb-2017-rev. a