



Juniper Networks Secure Access 제품은 Secure Access 2000 (SA 2000), Secure Access 4000 (SA 4000) 및 Secure Access (SA 6000)를 포함한 포괄적인 원격 액세스 어플라이언스를 통해 SSL VPN (Virtual Private Network) 시장을 선도하고 있습니다. 또한, SSL의 보안 기능과 표준 기반의 액세스 제어, 세분화된 정책 생성 및 탁월한 유연성을 모두 갖추고 있습니다. 따라서 엄격한 수준의 액세스 제어 옵션을 통해 모든 엔터프라이즈 작업에 대한 포괄적이고 광범위한 보안을 제공함으로써 가장 민감한 애플리케이션 및 데이터를 보호할 수 있습니다. Juniper Networks Secure Access 어플라이언스는 기존 IPSec 클라이언트 솔루션에 비해 저렴한 TCO의 강점과 독보적인 엔드-투-엔드 보안 기능을 자랑합니다.

주니퍼 네트워크스 Secure Access 어플라이언스

제품 설명

Juniper Networks SA 2000, SA 4000 및 SA 6000 SSL VPN 어플라이언스는 규모에 관계 없이 모든 기업의 요구를 충족합니다. Juniper Networks Secure Access 어플라이언스는 모든 표준 웹 브라우저의 공통 보안 프로토콜인 SSL을 사용하는 IVE (Instant Virtual Extranet) 플랫폼을 기반으로 개발되었습니다. SSL을 사용하는 경우, 클라이언트 소프트웨어의 사전 설치나 내부 서버의 변경, 막대한 비용 부담이 발생하는 지속적인 유지 보수 및 데스크톱 지원 등이 필요하지 않습니다. Juniper Networks Secure Access 어플라이언스는 인프라스트럭처 변경, DMZ 구축 및 소프트웨어 에이전트 설치 없이도 차별화된 사용자 및 그룹에 제어된 액세스를 지원하는 고급 파트너/고객 엑스트라넷 기능을 제공합니다.

아키텍처 및 주요 구성 요소

Juniper Networks SA 2000 SSL VPN은 SMB (Small-to-Medium Business)가 인터넷 보안은 물론, 비용 효과적인 원격 및 엑스트라넷 액세스를 구축할 수 있도록 지원합니다. 사용자는 웹상의 모든 시스템에서 기업 네트워크 및 애플리케이션에 액세스할 수 있습니다. SA 2000은 유연한 사용자 페일오버 기능과 고가용성을 제공합니다.

Juniper Networks SA 4000 SSL VPN을 통해 중/대규모 기업들은 웹 브라우저에서 비용 효과적인 방식으로 원격 및 파트너 엑스트라넷에 액세스할 수 있습니다. 이 어플라이언스는 안전한 고객/파트너 엑스트라넷을 구축할 수 있도록 풍부한 액세스 권한 관리 기능을 지원합니다. 이 기능을 사용할 경우 엔터프라이즈는 기업 인프라에 대한 액세스도 보호할 수 있으며, 이를 통해 다양한 직원 및 방문자들이 자신에게 필요한 리소스를 정확하게 활용하는 동시에 기업 보안 정책을 준수할 수 있습니다. 모든 유형의 트래픽에 대한 압축 기능이 내장되어 있어 속도를 더욱 가속화하며, 성능 요구치가 높은 환경의 경우에는 소프트웨어 라이선스를 통해 하드웨어 기반 SSL 가속화 기술을 사용할 수 있습니다. SA 4000 유연한 사용자 페일오버 기능과 고가용성을 제공합니다.

Juniper Networks SA 6000 SSL VPN은 대규모 엔터프라이즈 및 서비스 제공업체를 위해 설계된 맞춤형 제품으로서, 보안 액세스 및 인증 요구 수준이 높은 기업을 위한 동급 최강의 성능, 확장성 및 이중화 기능을 갖추고 있습니다. 최대 2500명에 달하는 동시 사용자 (직원, 비즈니스 파트너 및 고객)에게 안전한 원격 액세스를 제공하며, 멀티유닛 클러스터에 구축할 경우 HA (High Availability) 및 원활한 사용자 페일오버를 제공할 수 있어 보다 많은 사용자를 지원하도록 확장할 수 있습니다. SA 6000 하드웨어 플랫폼은 핫 스왑 교체 가능한 이중화 하드 디스크, 전원 공급장치 및 팬은 물론, 이중화 또는 메시 (Mesh) 구성을 위한 GBIC 기반의 다중 Ethernet 포트 등을 비롯한 제공 옵션을 통해 최대 규모의 엔터프라이즈급 시스템으로도 확장할 수 있으며 애플리케이션 제어를 최적화하도록 설계되었습니다. 또한, CPU 집약적인 암호화/복호화 프로세스를 가속화할 수 있는 최첨단 SSL 가속화 칩셋을 장착한 것은 물론, 모든 트래픽에 대한 압축 기능을 내장하고 있습니다.

기능 및 이점

Secure Access 6000 SSL VPN의 고가용성 지원

SA 6000은 네트워크에 접속하는 수 천명의 리모트 유저들을 지원할 수 있는 능력을 제공함으로써 대기업과 서비스 사업자의 증가하는 요구사항을 만족시킬 수 있도록 설계되었습니다. 다음은 SA 6000 플랫폼 상에서 지원할 수 있는 동시 사용자의 수를 보여줍니다.

- SA 6000 한 대 : 최대 5,000 명의 동시 사용자 지원
- SA 6000 장비 2 대 클러스터 : 최대 8,000 명의 동시 사용자 지원
- SA 6000 장비 3 대 클러스터 : 최대 12,000 명의 동시 사용자 지원
- SA 6000 장비 4 대 클러스터 : 최대 15,000 명의 동시 사용자 지원

고객 네트워크의 트래픽 시뮬레이션을 통해 실제 환경의 시나리오를 기반으로 한 성능 테스트를 모두 마쳤습니다. 코어 액세스의 경우 HTML 리라이팅과 정책 평가가 수반되는 실제 웹 애플리케이션들이 테스트되었습니다.

완벽한 다계층 보안

SA 2000, SA 4000 및 SA 6000은 다음과 같이 단말 장치 클라이언트, 장비, 데이터 및 서버 계층 보안 제어를 포함해 완벽하고 포괄적인 다계층 보안을 제공합니다.

특징	특징 설명	이점
Host Checker	세션 개시 이전과 세션 도중에 클라이언트 컴퓨터를 검사함으로써 설치된/작동 중인 단말 장치 보안 애플리케이션 (바이러스 차단, 방화벽 및 X 차단)을 요구하는 허용 가능한 장비 보안 상태 검증, 열려진/폐쇄된 포트 확인, 파일/프로세스 검사, Message Digest 5 (MD5) 해시 체크섬을 통해 진위 검증 등을 포함한 기본 제공되는 맞춤형 검사 기능을 지원함으로써 레지스트리 설정값, 시스템 인증서 등 확인	액세스 허용에 앞서 단말 장치의 기업 보안 정책 요구 사항 충족 여부 확인/보장, 필요할 경우 장비 치료 수행
Host Checker API	등급 최강의 단말 장치 보안 벤더와 함께 협력해 개발. 엔터프라이즈가 개인 방화벽, 바이러스 백신 클라이언트 또는 기타 보안 클라이언트가 설치된 관리 PC에 단말 장치 트러스트 정책을 적용하고 정책을 준수하지 않는 장비를 격리할 수 있도록 지원	원격 사용자 및 장비를 통한 최신 보안 정책 활용, 보다 손쉬운 관리 수행
Host Checker에서 TNC (Trusted Network Connect) 지원	안티바이러스에서 패치 관리, 규제 준수 관리 솔루션에 이르기까지 다양한 엔드포인트 보안 솔루션들의 상호운영성 보장	고객이 기존의 써드 파티 벤더 엔드포인트 보안 솔루션에 대한 투자를 활용할 수 있게끔 보장
정책 기반 보안 적용	엔터프라이즈가 맞춤형 API 애플리케이션을 작성하거나 고객 또는 파트너와 같이 다른 보안 클라이언트를 실행하는 외부 사용자의 액세스를 차단하지 않고도 비API 규격 호스트에 대한 신뢰를 구축할 수 있도록 지원	엔터프라이즈의 보안 클라이언트와 다른 클라이언트를 작동하는 파트너의 엑스트라넷 장비 (예: PC)에 대한 액세스를 지원
강화된 보안 어플라이언스 및 웹 서버	CyberTrust 및 iSec 파트너 (CC (Common Criteria) 인증)를 포함한 타사 보안 전문가의 포괄적 감사를 통해 한층 강화된 보안 인프라스트럭처	그 어떤 추가 서비스를 실행할 필요가 없도록 설계되었다는 점에서 공격 당할 위험이 낮음. 악용되거나 해킹 당할 백도어가 없음
커널 수준의 패킷 필터링 및 보안 라우팅을 채용한 보안 서비스	원치 않는 트래픽은 TCP 스택이 처리하기 전에 삭제됨 (drop)	이상 패킷이나 DOS 공격과 같이 인증되지 않은 연결 시도를 필터링함
SVW (Secure Virtual Workspace) (고급 소프트웨어 기능 세트)	관리되지 않는 PC 상에 데이터를 복사, 인쇄 또는 저장하지 못하도록 막는 원격 세션을 위한 별도의 보안 환경	사용자가 키오스크나 여타 관리되지 않는 단말 장치에서 기업 데이터에 액세스할 때 데이터 기밀성을 완벽하게 보장
Cache Cleaner	세션 도중에 설치된 모든 프록시 다운로드 및 Temp 파일을 로그아웃 시 삭제	단말 장치에 민감할 수 있는 세션 데이터가 남지 않도록 보장
데이터 트랩 및 캐시 제어	Non-Cacheable 형식으로 콘텐츠 렌더링	민감한 메타 데이터 (쿠키, 헤더, 양식 입력값)가 네트워크에 남지 않도록 보장
통합 악성 코드 보호	사전 설치된 검사 기능을 통해 키로거, 트로이 목마 및 원격 제어 애플리케이션으로부터 사용자 및 장비 보호	고객이 단말 장치 감염 억제 기능을 프로비저닝할 수 있도록 지원
위험 관리 조정	주니퍼의 SA SSL VPN 및 IDP (Intrusion Detection and Prevention) 어플라이언스는 IDP의 위험 탐지 기능을 통해 SSL VPN의 세션 ID를 위험 탐지 기능과 연계함으로써 공격 개시 사용자에게 자동 조치 실행	원격 액세스 트래픽 내에서 네트워크 수준 및 애플리케이션 수준 위험을 효과적으로 파악, 차단 및 치료

TCO절감

SA 2000, SA 4000 및 SA 6000은 엔터프라이즈급 보안 이점 외에도 TCO를 낮출 수 있는 풍부한 기능을 갖추고 있습니다.

특징	특징 설명	이점
SSL 사용	애플리케이션 계층에서의 웹 연결을 통해 원격 사용자와 내부 리소스 간의 보안 연결 설정	클라이언트 소프트웨어 구축, 유지 보수 및 기존 서버에 대한 변경 없이, 방화벽 프록시 및 NAT (Network Address Translation) 통과 (Traversal) 문제 없이 안전한 원격 액세스
업계 표준 프로토콜 및 보안 메소드 기반	전용 프로토콜을 설치하거나 구축할 필요가 없음	시간 경과에 따라 많은 애플리케이션 및 리소스 전반에서 SA 어플라이언스에 대한 투자를 활용할 수 있음
포괄적인 디렉토리 통합 및 광범위한 상호 운영성	인증 및 권한 부여를 위해 고객 네트워크의 기존 디렉토리를 활용할 수 있어 보안 정책을 재작성하지 않고도 세분화된 보안 액세스 가능	인프라스트럭처 변경 없이 기존 디렉토리 활용 가능 - 모든 디렉토리가 기본 제공/내장 디렉토리이기 때문에 통합을 위한 API는 필요하지 않음
강력한 인증, 아이덴티티, 액세스 관리 플랫폼의 통합	SecurID, SAML, PKI/디지털 인증 지원	기존의 기업 인증 방식들을 활용함으로써 관리 단순화
다중 호스트 이름 지원 (고급 소프트웨어 기능 세트)	단일 SA 어플라이언스로서 일단의 여러 가상 엑스트라넷 웹 사이트 호스팅	점진적으로 증설되는 서버 비용 및 관리 오버헤드 절감, 차별화된 엔트리 URL을 통해 투명한 사용자 경험 제공
사용자 정의 가능한 사용자 인터페이스 (고급 소프트웨어 기능 세트)	완벽하게 사용자 정의된 사용자 인증 페이지 생성	특정 역할에 대한 개인화된 화면을 제공함으로써 보다 효율적인 사용자 경험 보장
Juniper Networks Central Manager (고급 소프트웨어 기능 세트)	단일 장비/클러스터 내에서, 또는 글로벌 클러스터 구축 전반에서 SA 어플라이언스 구성, 업데이트 및 모니터링할 수 있는 직관적인 웹 기반 UI 지원	단일 중앙 지점에서 SA 어플라이언스를 손쉽게 관리, 구성 및 유지 보수
ICE (In Case of Emergency)	재난 또는 전염병 발생 시 한정 기간 동안 SA SSL VPN 어플라이언스에 대한 대규모 추가 사용자에게 라이선스 제공	예상치 못한 상황이 발생했을 때 기업이 지속적으로 업무 생산성을 유지하고, 협력 관계를 유지하며, 고객에 대한 지속적인 서비스를 제공함으로써 지속적인 업무 운영을 수행할 수 있도록 지원
크로스 플랫폼 지원	모든 플랫폼이 리소스 (예 : Windows, Mac, Linux, 모바일 장비)에 대한 액세스 권한을 획득할 수 있도록 지원	사용자가 운영 체제 유형에 관계 없이 모든 유형의 장비에서 기업 리소스에 액세스할 수 있는 유연성 제공

다양한 액세스 권한 관리 기능

SA 2000, SA 4000 및 SA 6000은 인프라스트럭처 변경, 맞춤형 개발 또는 소프트웨어 구축/유지 보수 등을 수행할 필요 없이 동적 액세스 권한 관리 기능을 제공합니다. 따라서, 안전한 원격 액세스는 물론, 안전한 엑스트라넷 및 인트라넷을 손쉽게 구축 및 유지할 수 있습니다. SA 어플라이언스에 로그인한 사용자는 인증 전 평가 단계를 거쳐 설정된 네트워크, 장비, ID 및 세션 정책 값을 통합한 세션 역할에 동적으로 대응됩니다. 또한, 세분화된 리소스 권한 부여 정책을 통해 보안 제약 조건을 정확하게 준수할 수 있습니다.

특징	특징 설명	이점
복합적인 역할/리소스 기반 정책 모델	관리자의 액세스 구성이 가능	보안 정책에 변화하는 비즈니스 요구 사항을 반영
인증 전 평가	로그인 허용에 앞서 Host Checker/Cache Cleaner 설치 여부를 포함한 네트워크 및 장비 속성, 단말 장치 보안 검사 결과, 소스 IP, 브라우저 유형 및 전자 인증서에 대한 검토 가능	동적 정책 적용 의사 결정에서 활용되는 평가 결과
동적 인증 정책	관리자가 각 고유 세션에 대한 동적 인증 정책을 설정할 수 있도록 지원	디렉토리, PKI 및 강력한 인증에 대한 엔터프라이즈의 기존 투자 활용
동적 역할 매핑	네트워크, 장비 및 세션 속성을 결합해 허용되는 3가지 유형의 액세스 결정	관리자가 각 고유 세션에 대해 목적별로 프로비저닝을 수행할 수 있도록 지원
리소스 권한 부여	URL, 서버 또는 파일 수준에 따라 고도로 세분화된 액세스 제어	관리자가 필수 데이터에 대한 액세스만을 제공하는 등 특정 그룹에 대한 보안 정책을 정의할 수 있도록 지원
세분화된 감사 및 로깅	보안 목적 및 용량 계획에 따라 사용자/리소스/이벤트 수준별 구성 가능	명확하고 이해하기 쉬운 형식으로 수행되는 세분화된 감사 및 로깅 기능
맞춤 표현식 (고급 소프트웨어 기능 세트)	역할 정의/매핑 규칙 및 리소스 권한 부여 정책 수준에서 "세션별" 속성의 동적 결합 지원	한층 강화된 정책 역할의 세분화 및 커스터마이징

사용자 셀프 서비스

SA 2000, SA 4000 및 SA 6000은 포괄적인 암호 관리 기능을 제공합니다. 이들 기능으로 최종 사용자 생산성을 높이고 다양한 사용자 리소스에 대한 관리를 대폭 간소화하며 헬프 데스크 통화 수를 크게 줄일 수 있습니다.

특징	특징 설명	이점
암호 관리 통합	디렉토리 스토어 (LDAP, Microsoft Active Directory, NT 등) 내 암호 정책에 포괄적으로 통합할 수 있는 표준 기반 인터페이스	사용자 인증을 위해 기존 서버 활용, 사용자가 새로운 사용자 이름 및 암호를 숙지하지 못하고 있는 경우에도 네트워크 액세스 가능
웹 기반 SSO (Single Sign-On) 기본 인증 및 NTLM	사용자가 로그인 인증서를 재입력하지 않고도 다른 액세스 관리 시스템에 의해 보호되는 기타 애플리케이션 및 리소스를 액세스할 수 있도록 지원	최종 사용자가 웹 기반 및 Microsoft 애플리케이션을 위해 여러 인증서를 입력하고 유지 관리할 필요가 없음
웹 기반 SSO Form 기반, 헤더 변수 기반, SAML 기반 (고급 소프트웨어 가능 세트)	사용자 이름, 인증서 및 기타 고객이 정의한 속성을 다른 제품의 인증 형식으로 전달하거나, 헤더 변수로서 전달 가능	사용자 생산성 향상 및 커스터마이징된 경험 제공

목적별 프로비저닝

SA 2000, SA 4000 및 SA 6000에는 3가지 액세스 메소드가 포함되어 있습니다. 사용자 역할에 따라 서로 다른 메소드를 선택할 수 있기 때문에 관리자는 엔터프라이즈의 보안 정책과 함께 계정 사용자, 장비 및 네트워크 속성을 고려해 세션별로 적절한 액세스 권한을 부여할 수 있습니다.

특징	특징 설명	이점
클라이언트리스 코어 웹 액세스	소켓 연결이 필요한 복잡한 JavaScript, XML, 또는 플래시 기반의 애플리케이션 및 Java 애플릿을 포함한 웹 기반 애플리케이션은 물론, 표준 기반 e-메일, Windows 및 UNIX 파일 공유, telnet/SSH 호스팅 애플리케이션, Citrix 및 Windows 터미널 서비스, 터미널 에뮬레이션 등에 대한 액세스	휴대용 장비를 비롯해 다양한 최종 사용자 시스템에서 가장 손쉽게 액세스할 수 있는 형식의 애플리케이션 및 리소스 액세스 제공, 고도로 세분화된 보안 제어 옵션 지원
SAM (Secure Application Manager) (SAMNC 라이선스)	클라이언트/서버 애플리케이션에 대한 액세스를 지원하는 경량형 Java 또는 Windows 기반 다운로드	웹 브라우저만을 사용한 클라이언트/서버 애플리케이션에 대한 액세스 지원, 별도의 클라이언트를 사전에 설치할 필요 없이 터미널 서버 애플리케이션에 대한 액세스 기본 제공
Network Connect (NC) (SAMNC License)	자동 프로비저닝된 크로스 플랫폼 다운로드를 통한 완벽한 네트워크 계층 연결, 도메인 SSO를 위한 Windows Logon/GINA 통합, 관리 권한에 대한 요구를 완화하기 위한 Installer Services 등 제공	사용자는 오직 웹 브라우저만 필요하며, Network Connect 모든 네트워크 환경에 최고 수준의 성능을 자동 제공하기 위해 2가지 가능한 전송 방식 가운데 하나를 투명하게 선택하며, Juniper Installer Services와 함께 사용할 경우 관리 권한 없이도 Network Connect를 설치, 실행 및 업그레이드 할 수 있을 뿐만 아니라 독립형 설치 옵션도 제공됨

제품 옵션

SA 2000, SA 4000 및 SA 6000은 제품에 추가할 수 있는 몇 가지 하드웨어 및 소프트웨어 옵션을 구비하고 있습니다.

첨단 단말 장치 보호 : Malware Protection 통합 옵션

첨단 단말 장치 보호 : Malware Protection은 Host Checker에 통합된 단말 장치 보안 소프트웨어 모델로서, 최종 사용자가 원격 액세스 세션을 시작하려고 하는 단말 장치 상에 상주하는 트로이 목마 및 키로거와 같은 원치 않는 악성 코드를 차단합니다. 악성 코드 모듈은 Host Checker 모듈로 구성되며 소프트웨어를 사전 설치하지 않아도 최종 사용자의 PC에 동적 제공됩니다. 모든 Secure Access 어플라이언스에는 25명의 동시 사용자에 대한 무료 라이선스가 포함되어 있습니다. 보다 많은 사용자를 지원할 수 있도록 이 기능을 향상시키고 싶은 고객들은 추가 라이선스를 구입해야 합니다.

첨단 단말 장치 보호 : Malware Protection 통합 업그레이드는 SA 2000, SA 4000 및 SA 6000에서 지원됩니다.

SAC (Secure Application Manager) 및 NC (Network Connect) 업그레이드 옵션

SSL VPN을 위한 Juniper Networks Core Clientless 액세스와 더불어 SAM 및 NC 업그레이드가 지원됩니다. SAM 및 NC는 SAM을 사용하는 클라이언트/서버 애플리케이션에 크로스 플랫폼을 지원하는 것은 물론, NC에서 볼 수 있는 적응형 이중 전송 방식을 이용해 완벽한 네트워크 계층 액세스를 제공합니다. SAM 및 NC를 Core Clientless 액세스와 결합할 경우, 모든 네트워크에서 광범위한 장비를 사용해 원격/이동 작업자에서 파트너/고객에 이르기까지 거의 모든 사용자에게 안전하게 액세스할 수 있습니다. SAM 및 NC는 2가지 액세스 방식을 제공하지만 관리자는 모든 구축 시나리오에서 각 사용자에게 할당하고 싶은 액세스 방식이나 액세스 방식의 조합을 정확하게 지정할 수 있습니다. 따라서, 관리자는 목적에 따라 프로비저닝을 수행함으로써 보안 요구와 액세스 요구 간의 조화를 유지할 수 있습니다. 동적 액세스 제어는 사용자, 단말 장치 및 네트워크 기준의 변화에 따라 액세스를 변경할 수 있도록 지원합니다.

SAMNC 업그레이드는 SA 2000, SA 4000 및 SA 6000에서 지원됩니다.

고급 기능 세트

Secure Access 어플라이언스에는 SMB 직원을 위한 원격 액세스 시스템부터 최대 규모의 글로벌 엔터프라이즈 엑스트라넷에 이르기까지 모든 기업의 요구를 충족하는 저렴한 솔루션을 개발할 수 있도록 설계된 기본 또는 고급 기능 세트가 제공됩니다. 어플라이언스와 함께 제공되는 기본 (Baseline) 기능은 엔터프라이즈가 안전한 원격 액세스를 구축하기 위해 필요한 기능을 제공하는 것은 물론 기본적인 고객/파트너 엑스트라넷 또는 인트라넷을 위한 프로비저닝을 지원합니다. 고급 기능 세트는 다양한 사용자 및 유스 케이스에서 보다 복잡한 시스템의 요구를 충족하는 고급 추가 기능을 제공하며, **Secure Access** 어플라이언스를 손쉽게 구성, 업데이트 및 모니터링할 수 있도록 설계된 직관적인 웹 기반 UI를 갖춘 강력한 제품인 **Secure Access Central Manager**도 그 하나입니다. 두 기능 모두 클라이언트 소프트웨어, 서버 변경, DMZ 구축 또는 소프트웨어 에이전트 구축 없이도 원격 액세스, 엑스트라넷 및 인트라넷 기능을 제공합니다. 다음은 고급 기능의 예입니다.

- 다중 루트를 임포트하고 CA, OSCP 및 다중 서버 인증서를 중개할 수 있는 기능을 포함한 고급 PKI 지원 기능
- 사용자 셀프 서비스
- 액세스 관리 통합
- 다중 호스트 이름 지원
- 커스터마이징 가능한 UI
- 유연한 동적 “세션별” 정책을 위해 Boolean 표현식을 이용한 속성 통합
- Boolean 표현식을 이용한 고급 역할 정의 및 역할 대응 규칙과 속성 통합
- Boolean 표현식을 이용한 고급 리소스 권한 부여 정책과 속성 통합
- 개별 작업 수준에서 구성 가능한 역할 기반 위임
- 유연한 역할 정의
- Juniper Networks Central Manager
- SVW (Secure Virtual Workspace)

고급 기능 업그레이드는 SA 2000, SA 4000 및 SA 6000에서 지원됩니다.

Secure Meeting 옵션

Secure Meeting 업그레이드 라이선스는 언제 어디서나 안전하면서도 비용 효과적인 온라인 웹 컨퍼런스 및 원격 제어 PC 액세스를 제공함으로써 Juniper Networks **Secure Access** 어플라이언스의 기능을 확장합니다. **Secure Meeting**은 실시간 애플리케이션 공유를 지원함으로써 인증을 받은 직원 및 파트너가 손쉽게 온라인 회의 일정을 설정하는 것은 물론, 교육 솔루션이나 특별한 솔루션 없이도 즉시 사용할 수 있는 직관적인 웹 인터페이스를 통해 인스턴트 메시징을 통한 회의를 개시할 수 있도록 합니다. 헬프 데스크 직원이나 고객 서비스 담당자는 소프트웨어 설치 없이도 사용자의 PC를 원격 제어함으로써 모든 사용자 또는 고객에게 계속해서 원격 지원을 제공할 수 있습니다. 기업들은 동급 최강의 AAA (Authentication, Authorization, and Accounting) 기능을 통해 **Secure Meeting**을 기존 내부 인증 인프라스트럭처 및 정책에 손쉽게 통합할 수 있습니다. 모든 트래픽을 위해 한층 강화된 주니퍼의 업계 선도적인 CC (Common Criteria) 인증 SSL VPN 어플라이언스 아키텍처 및 SSL/HTTPS 전송 보안을 토대로 관리자들은 웹 컨퍼런스 및 원격 제어 솔루션이 최상의 엔터프라이즈 보안 요구 사항을 준수하도록 할 수 있습니다.

Secure Meeting 업그레이드는 SA 2000, SA 4000 및 SA 6000에서 지원됩니다.

IVS (Instant Virtual System) 옵션

Juniper Networks Instant Virtual System (IVS) 옵션은 관리자들이 단일 어플

라이언스/클러스터 내에서 논리적으로 독립된 225개의 SSL VPN 게이트웨이를 프로비저닝할 수 있도록 설계되었습니다. 따라서, 서비스 제공업체들은 단일 장비/클러스터에서 여러 고객에게 네트워크 기반의 SSL VPN 매니지드 서비스를 제공할 수 있으며 엔터프라이즈는 여러 그룹 간에 SSL VPN 트래픽을 완벽하게 분리할 수 있습니다. IVS를 통해 완벽한 사용자 구분을 수행하는 것은 물론, 세분화된 역할 기반 VLAN (802.1Q) 태깅을 이용해 여러 고객 간에 트래픽을 분리할 수 있습니다. 따라서, 두 고객이 중복된 IP 주소를 가지고 있는 경우에도 최종 사용자의 트래픽을 안전하게 분리할 수 있으며 고객 기업의 원격 직원 및 파트너와 같이 서로 다른 사용자 구성에 대해서도 고유의 VLAN을 프로비저닝할 수 있습니다. DNS/WINS, AAA, 로그/어카운팅 서버 및 애플리케이션 서버 (웹 메일, 파일 공유 등)는 해당 고객의 인트라넷이나 서비스 제공업체 네트워크에 상주할 수 있습니다. 서비스 제공업체들은 원격 직원, 계약자, 파트너 등 서로 다른 대상에게 트래픽을 분배할 수 있는 유연성을 바탕으로 고객별로 전체 동시 사용자 수를 프로비저닝할 수 있습니다.

IVS 업그레이드는 SA 4000 및 SA 6000에서 지원됩니다.

HA (High Availability) 옵션

주니퍼 네트워크는 **Secure Access** 어플라이언스를 지원하는 다양한 HA 클러스터링 옵션을 개발함으로써 흔히 않는 시스템 장애 상황에서도 이중화와 완벽한 페일오버를 보장합니다. 또한, 이러한 클러스터링 옵션은 성능 요구치가 가장 높은 사용 시나리오를 처리할 수 있는 성능 확장성도 제공합니다. **Secure Access 2000** 및 **4000**을 클러스터 쌍으로 구입하고 **Secure Access 6000**을 멀티유닛 클러스터나 클러스터 쌍으로 구입하여 완벽한 이중화와 광범위한 사용자 확장성을 제공할 수 있습니다. 멀티유닛 클러스터 및 클러스터 쌍은 LAN 및 WAN에서 Stateful 피어링 기법을 통해 페일오버를 수행하기 때문에 하나의 유닛에 장애가 발생한 경우에도 시스템 구성 (인증 서버, 권한 부여 그룹, 북마크 등을 포함), 사용자 프로파일 설정값 (사용자 정의 북마크, 쿠키 등을 포함) 및 사용자 세션이 보존됩니다. 이와 같이 원활한 페일오버를 통해 사용자/엔터프라이즈 생산성에 영향이 미치지 않는 것은 물론, 사용자가 재로그인할 필요가 없으며 다운타임도 발생하지 않습니다. 멀티유닛 클러스터는 Active/Active 모드로 자동 구축되는 반면, 클러스터 쌍은 Active/Active 또는 Active/Passive 모드 중 하나로 구성할 수 있습니다.

HA 옵션은 SA 2000, SA 4000 및 SA 6000에서 지원됩니다.

ICE 옵션

SSL VPN은 허리케인, 테러 공격, 운송 파업, 전염병 또는 바이러스 출현과 같이 예측할 수 없는 최악의 상황에서도 사람들을 연결함으로써 기관 및 기업들이 중단 없이 업무를 수행할 수 있도록 도와줍니다. 오랜 기간 동안 전체 지역 또는 그룹을 격리할 덕분에 가능한 결과입니다. 위험과 비용 간에 최적의 균형을 유지하는 새로운 Juniper Networks **Secure Access ICE** 솔루션은 원격 액세스에 대한 갑작스러운 요구 증가에 대처할 수 있는 실시간 솔루션을 제공함으로써 재난 사고가 발생한 경우에도 무중단 업무 운영을 보장합니다. ICE는 한정 기간 동안 **Secure Access SSL VPN** 어플라이언스상의 대규모 추가 사용자에게 라이선스를 제공합니다. ICE는 기업에 다음과 같은 이점을 제공합니다.

- 직원들이 언제 어디서나 모든 장치를 이용해 애플리케이션 및 정보에 액세스할 수 있는 유비쿼터스 환경 구축으로 지속적인 생산성 유지
- 기업 리소스에 대한 철저한 보안 및 보호가 이루어진다는 것을 확인할 수 있는 한편, 애플리케이션 및 서비스에 대한 1년 365일 하루 24시간 실시간 액세스를 통한 협력 관계 지속

- 온라인 협업을 통해 고객 및 파트너에게 탁월한 서비스를 지속적으로 제공
- 긴급 상황 및 COOP와 관련한 연방/정부 규제 준수
- 위험 및 확장성과 구축 비용 및 용이성 간의 균형 유지

ICE 라이선스는 SA4000 및 SA6000에서 지원되며 다음과 같은 기능을 포함하고 있습니다.

- 기본 모델
- 고급 모델
- SAM (Secure Application Manager) 및 NC (Network Connect)
- Secure Meeting
- SSL 가속화

사양	SA 2000	SA 4000	SA 6000
크기 및 전원			
크기 (H x W x D)	16.7" in x 1.74" in x 15" in (42.42 cm x 4.41 cm x 38.10 cm)	16.7" in x 1.74" in x 15" in (42.42 cm x 4.41 cm x 38.10 cm)	16.7" in x 3.5" in x 16.2" in (42.42 cm x 8.89 cm x 41.15 cm)
무게	13.2 lb(5.99 kg) 평균 (박스 제외)	13.6 lb(6.17 kg) 평균 (박스 제외)	28.5 lb(12.94 kg) 평균 (박스 제외)
랙마운트형	Yes, 19"	Yes, 19"	Yes, 19"
A/C 전원 공급장치	100-240 VAC, 50-60 Hz, 2.5 A (최대), 260 W	100-240 VAC, 50-60 Hz, 2.5 A (최대), 260 W	100-240 VAC, 50-60 Hz, 2.5 A (최대), 500 W
시스템 배터리	CR2032 3 V 리튬 코인 셀	CR2032 3 V 리튬 코인 셀	CR2032 3 V 리튬 코인 셀
효율성	65% minimum, full load	65% minimum, full load	65% minimum, full load
MTBF	87,000시간	70,000시간	78,000시간
소재	18 게이지 (.048") 냉연 철강	18 게이지 (.048") 냉연 철강	18 게이지 (.048") 냉연 철강
팬	1개의 블로어(blower), 1-40 mm 볼베어링 팬 (전원 공급장치)	3-40 mm 볼베어링 팬, 1-40 mm 볼베어링 팬 (전원 공급장치)	외부 접근이 가능하며 핫스왑 교체가 가능한 2개의 볼베어링 팬
패널 디스플레이			
프론트 패널 전원 버튼	Yes	Yes	Yes
전원 LED, HD 활동, 온도	Yes	Yes	Yes
PS Fail	No	No	Yes
HDD 활동 및 RAID 상태 LED	No	No	Yes
포트			
트래픽	2개의 RJ-45 Ethernet - 10/100/1000 전이중/반이중 (자동 협상)	2개의 RJ-45 Ethernet - 10/100/1000 전이중/반이중 (자동 협상)	2개의 RJ-45 Ethernet - 10/100/1000 전이중/반이중 (자동 협상) 2개의 SFP 포트 - Gig-E
관리	해당 사항 없음	해당 사항 없음	1개의 RJ-45 Ethernet-10/100/1000 전이중 또는 반이중 (자동 협상)
Fast Ethernet	IEEE 802.3u 호환	IEEE 802.3u 호환	IEEE 802.3u 호환
Gigabit Ethernet	IEEE 802.3z 또는 IEEE 802.3ab 호환	IEEE 802.3z 또는 IEEE 802.3ab 호환	IEEE 802.3z 또는 IEEE 802.3ab 호환
콘솔	1개의 9-핀 시리얼 콘솔 포트	1개의 9-핀 시리얼 콘솔 포트	1개의 9-핀 시리얼 콘솔 포트
환경			
운영 시 온도	50° ~ 95° F (10° C ~ 35° C)	50° ~ 95° F (10° C ~ 35° C)	50° ~ 104° F (10° C ~ 40° C)
보관 온도	-40° ~ 158° F (-40° C ~ 70° C)	-40° ~ 158° F (-40° C ~ 70° C)	-40° ~ 158° F (-40° C ~ 70° C)
상대 습도 (운영)	8% ~ 90% 비응축	8% ~ 90% 비응축	8% ~ 90% 비응축
상대 습도 (보관)	5% ~ 95% 비응축	5% ~ 95% 비응축	5% ~ 95% 비응축
고도 (운영)	-50 ~ 10,000 ft (3,000 m)	-50 ~ 10,000 ft (3,000 m)	-50 ~ 10,000 ft (3,000 m)
고도 (보관)	-50 ~ 35,000 ft (10,600 m)	-50 ~ 35,000 ft (10,600 m)	-50 ~ 35,000 ft (10,600 m)

사양	SA 2000	SA 4000	SA 6000
인증			
안전 인증	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
전자파 방출 인증	FCC Class A, VCCI Class A, CE Class A	FCC Class A, VCCI Class A, CE Class A	FCC Class A, VCCI Class A, CE Class A
CC (Common Criteria) EAL4 인증	Yes	Yes	Yes
FIPS 140-2, Level 3 인증	No	Yes	Yes
보증	90일 : 지원 계약을 통해 연장 가능	90일 : 지원 계약을 통해 연장 가능	90일 : 지원 계약을 통해 연장 가능

주문 정보

Secure Access 2000 Base System

SA2000 Secure Access 2000 Base System

Secure Access 2000 사용자 라이선스

SA2000-ADD-25U	SA 2000에 25명의 동시 사용자 추가
SA2000-ADD-50U	SA 2000에 50명의 동시 사용자 추가
SA2000-ADD-100U	SA 2000에 100명의 동시 사용자 추가

Secure Access 2000 기능 라이선스

SA2000-SAMNC	Secure Application Manager and Network Connect for SA 2000
SA2000-ADV	Advanced for SA 2000
SA2000-MTG	Secure Meeting for SA 2000
SA-AED-ADD-50U	첨단 단말 장치 보호 : 악성 코드 차단 - 50명의 동시 사용자 추가
SA-AED-ADD-100U	첨단 단말 장치 보호 : 악성 코드 차단 - 100명의 동시 사용자 추가

Secure Access 2000 클러스터링 라이선스

SA2000-CL-25U	클러스터링 : 타 SA 2000에서 25명의 추가 사용자를 공유할 수 있도록 지원
SA2000-CL-50U	클러스터링 : 타 SA 2000에서 50명의 추가 사용자를 공유할 수 있도록 지원
SA2000-CL-100U	클러스터링 : 타 SA 2000에서 100명의 추가 사용자를 공유할 수 있도록 지원

Secure Access 4000 Base System

SA4000 Secure Access 4000 Base System

Secure Access 4000 사용자 라이선스

SA4000-ADD-50U	SA 4000에 50명의 동시 사용자 추가
SA4000-ADD-100U	SA 4000에 100명의 동시 사용자 추가
SA4000-ADD-250U	SA 4000에 250명의 동시 사용자 추가
SA4000-ADD-500U	SA 4000에 500명의 동시 사용자 추가
SA4000-ADD-1000U	SA 4000에 1000명의 동시 사용자 추가

Secure Access 4000 기능 라이선스

SA4000-SAMNC	Secure Application Manager and Network Connect for SA 4000
SA4000-ADV	Advanced for SA 4000
SA4000-MTG	Secure Meeting for SA 4000
SA4000-SSL	SSL Acceleration License for SA 4000
SA4000-IVS	Instant Virtual System for SA 4000
SA-AED-ADD-50U	첨단 단말 장치 보호 : 악성 코드 차단 - 50명의 동시 사용자 추가
SA-AED-ADD-100U	첨단 단말 장치 보호 : 악성 코드 차단 - 100명의 동시 사용자 추가
SA-AED-ADD-250U	첨단 단말 장치 보호 : 악성 코드 차단 - 250명의 동시 사용자 추가
SA-AED-ADD-500U	첨단 단말 장치 보호 : 악성 코드 차단 - 500명의 동시 사용자 추가

Secure Access 4000 클러스터링 라이선스

SA4000-CL-50U	클러스터링 : 타 SA 4000에서 50명의 추가 사용자를 공유할 수 있도록 지원
SA4000-CL-100U	클러스터링 : 타 SA 4000에서 100명의 추가 사용자를 공유할 수 있도록 지원
SA4000-CL-250U	클러스터링 : 타 SA 4000에서 250명의 추가 사용자를 공유할 수 있도록 지원
SA4000-CL-500U	클러스터링 : 타 SA 4000에서 500명의 추가 사용자를 공유할 수 있도록 지원
SA4000-CL-1000U	클러스터링 : 타 SA 4000에서 1000명의 추가 사용자를 공유할 수 있도록 지원

Secure Access 6000 Base System

SA6000 Secure Access 6000 Base System

Secure Access 6000 사용자 라이선스

SA6000-ADD-100U	SA 6000에 100명의 동시 사용자 추가
SA6000-ADD-250U	SA 6000에 250명의 동시 사용자 추가
SA6000-ADD-500U	SA 6000에 500명의 동시 사용자 추가
SA6000-ADD-1000U	SA 6000에 1000명의 동시 사용자 추가
SA6000-ADD-2500U	SA 6000에 2500명의 동시 사용자 추가
SA6000-ADD-5000U*	SA 6000에 6000명의 동시 사용자 추가
SA6000-ADD-7500U*	SA 6000에 7500명의 동시 사용자 추가
SA6000-ADD-10000U*	SA 6000에 10000명의 동시 사용자 추가
SA6000-ADD-12500U*	SA 6000에 12500명의 동시 사용자 추가
SA6000-ADD-15000U*	SA 6000에 15000명의 동시 사용자 추가

*다중 SA 6000이 필요

Secure Access 6000 기능 라이선스

SA6000-SAMNC	Secure Application Manager and Network Connect for SA 6000
SA6000-ADV	Advanced for SA 6000
SA6000-MTG	Secure Meeting for SA 6000
SA6000-IVS	INSTANT VIRTUAL SYSTEM for SA 6000
SA-AED-ADD-50U	첨단 단말 장치 보호 : 악성 코드 차단 - 50명의 동시 사용자 추가
SA-AED-ADD-100U	첨단 단말 장치 보호 : 악성 코드 차단 - 100명의 동시 사용자 추가
SA-AED-ADD-250U	첨단 단말 장치 보호 : 악성 코드 차단 - 250명의 동시 사용자 추가
SA-AED-ADD-500U	첨단 단말 장치 보호 : 악성 코드 차단 - 500명의 동시 사용자 추가
SA-AED-ADD-1000U	첨단 단말 장치 보호 : 악성 코드 차단 - 1000명의 동시 사용자 추가
SA-AED-ADD-2500U	첨단 단말 장치 보호 : 악성 코드 차단 - 2500명의 동시 사용자 추가

주문 정보 (계속)

Secure Access 6000 클러스터링 라이선스

SA6000-CL-100U	클러스터링 : 타 SA 6000에서 100명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-250U	클러스터링 : 타 SA 6000에서 250명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-500U	클러스터링 : 타 SA 6000에서 500명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-1000U	클러스터링 : 타 SA 6000에서 1000명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-2500U	클러스터링 : 타 SA 6000에서 2500명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-5000U	클러스터링 : 타 SA 6000에서 5000명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-7500U	클러스터링 : 타 SA 6000에서 7500명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-10000U	클러스터링 : 타 SA 6000에서 10000명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-12500U	클러스터링 : 타 SA 6000에서 12500명의 추가 사용자를 공유할 수 있도록 지원
SA6000-CL-15000U	클러스터링 : 타 SA 6000에서 15000명의 추가 사용자를 공유할 수 있도록 지원

액세서리

S6000-PS	현장 업그레이드가 가능한 보조 전원 공급장치 – SA 6000용
S6000-HD	현장 업그레이드가 가능한 보조 하드 디스크 – SA 6000용
S6000-MEM	인증된 VAR을 통해서만 현장 업그레이드가 가능한 2 GB 추가 메모리 – SA 6000D용
S6000-FAN	현장 교체 가능한 팬 – SA 6000용
SA-ACC-RCKMT-KIT-1U	예비용 Secure Access 랙 마운트 키트 – 1U
SA-ACC-RCKMT-KIT-2U	예비용 Secure Access 랙 마운트 키트 – 2U
SA-ACC-PWR-AC-USA	예비용 Secure Access AC 전원 코드 (USA)
SA-ACC-PWR-AC-UK	예비용 Secure Access AC 전원 코드 (영국)
SA-ACC-PWR-AC-EUR	예비용 Secure Access AC 전원 코드 (유럽)
SA-ACC-PWR-AC-JPN	예비용 Secure Access AC 전원 코드 (일본)
SA6000-GBIC-FSX	GBIC Transceiver – Fiber SX – SA 6000용
SA6000-GBIC-FLX	GBIC Transceiver – Fiber LX – SA 6000용
SA6000-GBIC-COP	GBIC Transceiver – Copper – SA 6000용

주니퍼 네트워크에 대하여

주니퍼 네트워크는 High-Performance Networking을 지향하는 네트워크 업계 선도적인 업체입니다. 주니퍼는 단일 네트워크 상에서 서비스와 애플리케이션 운용을 가속화 시킬 수 있는 신뢰성 있는 네트워크 환경 구축을 위해 High-Performance Network 인프라를 제공하는데 주력하고 있습니다. 이러한 High-Performance Network는 곧 고객에게 High-Performance 비즈니스가 가능하게 하는 원동력이 되고 있습니다. 추가 정보는 www.kr.juniper.net에서 확인할 수 있습니다.

