데이터 시트

Cisco Secure Access Control Server Version 3.3 (Windows용)

Cisco Secure Access Control Server는 신원 확인(identity) 기반의 광범위한 네트워킹 솔루션과 안전한 사용자 환경을 시스코의 지능 정보 네트워크에 제공합니다. 이 솔루션은 네트워크 인프라의 모든 기업 사용자, 관리자 및 자원을 통합하고 제어하는 역할을 합니다.

제품 개요

오늘날 네트워크 액세스 방법이 날로 향상됨에 따라 보안 침해와 통제되지 않은 사용자 액세스가 주요한 문제가 되고 있습니다. 인터넷 사용이 증가함에 따라 네트워크 관리자는 장치와 사용자 식별을 통해 안전한 트랜잭션을 보장하고 바이러스와 서비스 거부(DoS) 공격의 확산을 차단해야 하는 문제에 직면했습니다. 이러한 문제는 네트워크 경계뿐만 아니라 네트워크 내부에도 존재합니다. 또한 IEEE 802.11 무선 LAN과 항시 연결되는 고속 이더넷 연결이 광범위하게 채택됨에 따라 조직 네트워크 내에서 이러한 문제가 더 심화되게 되었습니다. 이렇듯 도처에 존재하는 보안 취약성을 줄이기 위해 신원 확인 네트워킹 기술에 투자하는 것은 운영 및 투자 회수 측면에서 볼 때 고려해 볼만 합니다.

이러한 역동적인 네트워크 변화와 보안 위협의 증가는 액세스 제어 관리 솔루션 분야에 새로운 기회를 제공했습니다. 이제 공용 키 인프라 및 두 단계 인증과 같은 보다 강력해진 인증을 사용하여 공용 네트워크와 VPN에서 사용자의 회사 리소스 액세스를 제어할 수 있습니다. 네트워크 관리자는 유연한 인증 정책을 제공하는 솔루션을 원합니다. 이러한 유연한 인증 정책은 엔드포인트의 사용자에게 연결될 뿐만 아니라 사용자가 액세스하는 서비스 유형에도 연결되고 네트워크 액세스에 사용되는 시스템 유형에도 연결됩니다. 끝으로 네트워크 사용자의 동작을 추적하고 모니터링하여 귀중한 네트워크 리소스의 불필요한 사용과 과도한 사용을 막는 것이 매우 중요합니다.

이제 Cisco® Secure ACS(Access Control Server)에서 신원 확인 네트워킹을 사용하여 네트워크가 사용자별 또는 장치별로 서비스를 제공할 수 있습니다. Cisco Secure ACS는 확장성이 뛰어난 고성능의 액세스 제어 서버이며 중앙 집중식 RADIUS 서버 또는 TACACS+ 서버로 작동합니다. Cisco Secure ACS는 중앙 집중식 신원 확인 네트워킹 솔루션에서 인증, 사용자/관리자 액세스 및 정책 제어를 통합함으로써 액세스 보안을 강화하기 때문에 유연성이 더 향상되고 이동성과 보안 및 사용자의 생산성이 높아집니다. Cisco Secure ACS는 사용자 확장과 네트워크 관리 액세스에 관련된 운영 및 관리상의 부담을 덜어줍니다. Cisco Secure ACS는 모든 사용자 계정에 대해 중앙 데이터베이스를 사용하여 모든 사용자 권한을 중앙에서 제어하고 이 권한을 네트워크에 있는 수백, 수천 대의 액세스 포인트에 분배합니다. Cisco Secure ACS는 네트워크 사용자의 동작을 면밀하게 보고하고 모니터링할 뿐만 아니라, 전체 네트워크에서 액세스 연결 및 장치 구성에 관련된 모든 변경 사항을 기록함으로써 IT 운영 비용을 절감해 줍니다. Cisco Secure ACS는 유/무선 LAN, 전화 접속, 광대역, 컨텐츠, 스토리지, VoIP(Voice over IP), 방화벽 및 VPN을 비롯한 다양한 종류의 액세스 연결을 지원합니다.

Cisco Secure ACS는 Cisco IBNS(Identity-Based Networking Services) 아키텍처의 핵심 구성요소입니다. 네트워크 경계에서 액세스 제어가 관리되었던 경우, Cisco IBNS는 802.1X(포트 기반 네트워크 액세스 제어를 위한 IEEE 표준) 및 EAP(Extensible Authentication Protocol)와 같은 포트 보안 표준을 기반으로 하여 LAN 내에서 보안 인증, 권한 부여 및 계정 관리(AAA)를 확장합니다. 이 새로운 아키텍처에서는 사용자별 할당량, 가상 LAN(VLAN) 및 ACL 등의 새로운 정책 제어가 가능하며 인증 장치(스위치 또는 무선 액세스 포인트)가 RADIUS 클라이언트가 되어 AAA 서버에 이러한 제어를 요청할 수 있습니다.

Cisco Secure ACS는 또한 Cisco NAC(Network Admission Control)의 핵심 구성요소이기도 합니다. Cisco NAC는 시스코 시스템즈가 주도하는 멀티벤더 프로그램이며 바이러스 및 웜과 같은 보안 위협의 피해를 줄이는 것이 목적입니다. NAC를 사용하면, 신뢰할 수 있는 호환 가능한 엔드포인트 장치(예: PC, 서버 및 PDA)에만 네트워크 액세스를 허용하고 비호환 장치의 액세스는 제한할 수 있습니다. Cisco NAC는 시스코 자가 방어 네트워크(Self-Defending Network)의 첫 번째 단계이며 이후 단계의 기반이 됩니다. 이후 단계에서는 엔드포인트 및 네트워크 보안 호환성을 확장하여 동적인 감염 차단 성능을 제공합니다. NAC 혁신을 통해 호환 엔드포인트 또는 기타 시스템 구성요소에서 악의적 또는 감염된 시스템의 악용을 보고할 수 있습니다. NAC는 감염된 시스템을 나머지 네트워크로부터 동적으로 격리시켜주며 바이러스, 웜 및 복합적인 위협이 전파되는 것을 상당히 줄여줍니다.

Cisco Secure ACS는 WAN 또는 LAN 연결이 늘어나는 조직에게 다양한 고성능 및 확장성 기능을 제공하는 강력한 액세스 제어 서버입니다. 표 1은 Cisco Secure ACS의 이점을 나타냅니다.

표 1 Cisco Secure ACS 주요 이점

쉬운 사용성	웹 기반 사용자 인터페이스로 사용자 프로필, 그룹 프로필 및 Cisco Secure ACS 구성을 단순화하고 배포합니다.
확장성	Cisco Secure ACS는 리던던시형 서버, 원격 데이터베이스 및 사용자 데이터베이스 백업 서비스 지원을 통해 대규모 네트워크 환경을 지원하도록 설계되었습니다.
확장	확장 LDAP(Extensibility Lightweight Directory Access Protocol) 인증 포워딩은 Sun, Novell 및 Microsoft를 비롯한 주요 디렉토리 공급업체에서 제공하는 디렉토리에 저장된 사용자 프로필의 인증을 지원합니다.
관리	Windows Active Directory 및 Windows NT 데이터베이스 지원에서는 Windows 사용자 이름 및 암호 관리를 통합하며 실시간 통계 보기를 위해 Windows 성능 모니터를 사용합니다.
운영	각 Cisco Secure ACS 관리자에게 다른 액세스 수준을 제공함으로써 원활한 제어와 최대의 유연성을 통해 네트워크의 모든 장치에 대해 보안 정책을 시행하고 변경할 수 있습니다.
제품의 유연성	Cisco IOS® Software에는 AAA 지원이 포함되어 있기 때문에 시스코가 판매하는 Cisco Secure ACS를 거의 모든 네트워크 액세스 서버에서 사용할 수 있습니다. (Cisco IOS Software 릴리스가 RADIUS 또는 TACACS+를 지원해야 합니다.)
통합	Cisco IOS 라우터 및 VPN 솔루션과의 긴밀한 통합을 통해 Multichassis Multilink Point-to-Point Protocol 및 Cisco IOS Software 명령 권한 부여와 같은 기능을 제공합니다.
타사 지원	Cisco Secure ACS는 RFC 호환 RADIUS 인터페이스(예: RSA, PassGo, Secure Computing, ActiveCard, Vasco 및 CryptoCard)를 제공하는 모든 OTP(One-Time Password) 공급업체를 위해 토큰 서버 지원을 제공합니다.
제어	Cisco Secure ACS는 시간, 네트워크 사용, 기록된 세션 수 및 요일별 액세스 제한을 위해 동적인 할당량을 제공합니다.

ACS Version 3.3의 주요 기능

Cisco NAC 지원–Cisco Secure ACS 3.3은 NAC 배치 시에 정책 결정 포인트로 사용됩니다. 사용자가 구성한 정책을 사용하는 Cisco Secure ACS는 Cisco Trust Agent가 보낸 자격 증명을 평가하고 호스트의 상태를 결정한 후 이 호스트 상태에 적합한 AAA 클라이언트 ACL을 보냅니다. 호스트 자격 증명을 평가하여 특정한 여러 정책(예: 운영 체제 패치 수준 및 바이러스 차단 DAT 파일 버전)을 시행할 수 있습니다. Cisco Secure ACS는 모니터링 시스템에 사용할 수 있도록 정책 평가 결과를 기록합니다. 정책은 Cisco Secure ACS에 의해 로컬로 평가될 수 있으며 또한 Cisco Secure ACS가 전달한 자격 증명을 외부 정책 서버가 받아 평가한 후 반환되는 결과일 수도 있습니다. 예를 들어, 바이러스 차단 공급업체에 해당하는 자격 증명은 공급업체 바이러스 차단 정책 서버에 전달될 수 있습니다.

무선 인증을 위한 EAP-FAST(Flexible Authentication via Secure Tunneling) 지원– EAP-FAST는 공용 액세스가 가능한 새로운 IEEE 802.1X EAP 형식이며, 강력한 암호 정책을 시행할 수 없는 고객이나 802.1X EAP 형식(디지털 증명이 필요 없고, 다양한 종류의 사용자 및 암호 데이터베이스를 지원하고, 암호 만료 및 변경을 지원하고, 배치 및 관리가 쉽고 유연한 형식)을 배치하려는 고객을 지원하기 위해 개발되었습니다. 예를 들어, 강력한 암호 정책을 시행할 수 없고 인증을 사용하지 않으려는 Cisco EAP(Extensible Authentication Protocol) 사용 고객은 EAP-FAST로 마이그레이션하여 무차별적인 사전 공격을 차단할 수 있습니다. Cisco Secure ACS 3.3은 현재 시스코 호환 클라이언트 장치와 Cisco Aironet® 802.11a/b/g WLAN 클라이언트 어댑터에서 사용할 수 있는 EAP-FAST 신청을 지원합니다.

다운로드 가능한 IP ACL–Cisco Secure ACS Version 3.3에서는 이 기능을 지원하는 모든 레이어 3 네트워크 장치로 사용자별 ACL 지원을 확장합니다. 여기에는 Cisco PIX® Firewall, Cisco VPN 솔루션 및 Cisco IOS 라우터가 포함됩니다. 사용자별 또는 그룹별로 적용되는 ACL 세트를 정의할 수 있습니다. 이 기능은 올바른 ACL 정책을 시행할 수 있도록 함으로써 NAC 지원을 보완합니다. NAF와 함께 사용할 경우, 다운로드 가능 ACL을 AAA 클라이언트별로 다르게 적용할 수 있으며 이를 통해 사용자 및 액세스 장치별로 ACL을 고유하게 지정할 수 있습니다.

CRL(Certification Revocation List) 비교–Cisco Secure ACS 3.3에서는 X.509 CRL 프로필을 사용하여 인증서 취소 기능을 지원합니다. CRL은 취소된 인증서를 식별하기 위한 타임 스탬프가 찍힌 목록입니다. 이 목록은 인증 기관이나 CRL 발급 기관에서 서명하며 공용 리파지토리에서 무료로 사용할 수 있습니다. Cisco Secure ACS 3.3은 LDAP 또는 HTTP를 사용하여 CDP(CRL Distribution Point)에서 CRL을 주기적으로 검색하고 검색된 CRL을 EAP-TLS 인증 중에 사용하기 위해 저장합니다. EAP-TLS 인증 중에 사용자가 제공한 인증서가 검색된 CRL에 존재하는 경우, Cisco Secure ACS가 인증에 실패하고 사용자 액세스를 거부합니다. 이 기능은 빈번하게 변화하는 조직에서 매우 중요하며 네트워크 악용으로부터 소중한 회사 자산을 지켜줍니다.

MAR(Machine Access Restrictions)–Cisco Secure ACS 3.3에는 Windows 시스템 인증을 향상시켜주는 MAR가 있습니다. Windows 시스템 인증이 활성화되어 있는 경우 MAR를 사용하면 Windows 외부 사용자 데이터베이스에 인증하려는 EAP-TLS 및 Microsoft PEAP(Protected Extensible Authentication Protocol) 사용자의 권한 부여를 제어할 수 있습니다. 구성 가능한 시간 이내에 시스템 인증을 획득하지 못한 컴퓨터로 네트워크에 액세스하는 사용자에게는 지정된 사용자 그룹의 권한이 부여됩니다. 필요에 따라 이 사용자 그룹을 구성하여 권한 부여를 제한할 수 있습니다. 다른 방법으로, 네트워크 액세스를 완전히 거부할 수 있습니다.

NAF(Network Access Filtering)–Cisco Secure ACS 3.3에는 새로운 유형의 SPC(Shared Profile Component)로 NAF가 있습니다. NAF를 사용하면 네트워크 액세스 제한과 다운로드 가능 ACL을 AAA 클라이언트 이름, 네트워크 장치 그룹 또는 AAA 클라이언트의 IP 주소에 유연하게 적용할 수 있습니다. IP 주소별로 적용된 NAF는 IP 주소 범위와 와일드카드를 사용할 수 있습니다. 이 기능에서는 네트워크 액세스 제한과 다운로드 가능 ACL을 미세하게 적용할 수 있습니다. 이전에는 모든 장치에 동일한 액세스 제한이나 ACL를 사용할 수 있었습니다. NAF를 통해 유연한 네트워크 장치 제한 정책을 정의할 수 있으며 이것은 대규모 환경에서 일반적인 요구사항입니다.

Cisco Secure ACS Solution Engine상에 Cisco Security Agent 통합 –이제 Cisco Secure ACS 3.3 Solution Engine에는 독립형 Cisco Security Agent가 미리 설치되어 제공됩니다. 이러한 기본 장치 이미지와의 통합을 통해 Day Zero 공격으로부터 Cisco Secure ACS Solution Engine을 보호할 수 있습니다. Cisco Security Agent에서 제공하는 동작 기반의 새로운 기술을 사용하여 바이러스와 웜으로 인한 지속적인 위협으로부터 Cisco Secure ACS Solution Engine을 보호할 수 있습니다.

복제 기능 향상–이제 Cisco Secure ACS 3.3을 사용하여 사용자와 그룹 데이터베이스를 별도로 복제할 수 있습니다. 변경된 사용자 계정을 복제하기 위해 그룹을 자동으로 복제할 필요가 더 이상 없습니다. 마찬가지로 그룹을 복제하기 위해 사용자를 복제할 필요가 없습니다. 이러한 복제 기능 향상으로 인해 복제 이벤트 중에 Cisco Secure ACS 사이에 전송되는 데이터의 양이 줄어듭니다. 또한 Cisco Secure ACS 복제 파트너 사이의 느린 네트워크 연결을 위해 구성 가능한 복제 시간 제한 옵션이 추가되었습니다.

시스템 요구사항

Cisco Secure ACS는 Cisco Secure ACS Windows 및 Cisco Secure ACS Solution Engine의 두 옵션으로 제공됩니다. Cisco Secure ACS Solution Engine은 Cisco Secure ACS 라이센스가 미리 설치된 1-RU 보안 강화 장치입니다.

Cisco Secure ACS Windows 구현을 위해서는 Windows Server가 표 2에 나열된 최소 하드웨어 요구사항을 충족시켜야 합니다.

표 2 Cisco Secure ACS Windows의 최소 서버 사양

프로세서 속도	550 MHZ 이상
메모리	최소 256 MB RAM
하드 드라이브	최소 250 MB의 여유 디스크 공간
해상도	최소 800 x 600(256 컬러)

Cisco 1112 플랫폼에서 사용할 수 있는 Cisco Secure ACS Solution Engine의 사양은 표 3과 같습니다.

표 3 Cisco Secure ACS Solution Engine 서버 사양

프로세서 속도	Pentium IV, 3.2 GHz
메모리	1 GB RAM
하드 드라이브	80 GB의 빈 디스크 공간
인터페이스	내장형 10/100 이더넷 컨트롤러 2개, 플로피 디스크 드라이브 1개

주문 정보

Cisco Secure ACS는 전세계 시스코 판매 및 유통 채널을 통해 구입이 가능합니다. Cisco Secure ACS Windows에는 Microsoft Windows 워크스테이션상에 독립 설치하는 데 필요한 모든 구성요소가 포함됩니다. Cisco Secure ACS Solution Engine에는 Cisco Secure ACS 소프트웨어 라이센스가 미리 설치되어 제공됩니다. 제품 번호는 Cisco Secure ACS Version 3.3 제품 게시판(Product Bulletin)을 참조하십시오.

주문을 하려면 시스코 주문(Cisco Ordering) 홈 페이지를 방문하십시오.

서비스 및 지원

시스코는 고객의 성공을 촉진하기 위해 폭넓은 서비스 프로그램을 제공하고 있습니다. 이러한 혁신적인 서비스 프로그램들은 인력, 프로세스, 툴 및 파트너로 이뤄진 독특한 조합을 통해 제공되며 그 결과는 높은 고객 만족도로 나타납니다. 시스코 서비스는 여러분의 네트워크 투자를 보호하고, 네트워크 운영을 최적화합니다. 또한 새로운 애플리케이션을 도입하여 네트워크 인텔리전스와 비즈니스 영역을 확대할 수 있도록 네트워크 환경을 조성합니다. 시스코 서비스에 대한 자세한 정보는 시스코 기술 지원 서비스를 방문하십시오.

추가 정보

Cisco Secure ACS Version 3.3의 사용자 가이드와 릴리스 노트를 비롯하여 Cisco Secure ACS 3.3에 대한 자세한 내용은 http://www.cisco.com/go/acs를 방문하십시오.

제품 주문, 구입 가능 여부 및 지원 문의 정보에 대한 질문이 있으시면 제품 마케팅 그룹(ciscoworks@cisco.com)으로 전자메일을 보내주십시오.

www.cisco.com/kr

2005-07-15

■ Gold 파트너	• ㈜데이타크레프트 코리아	02-6256-7000	• ㈜인네트	02-3451-5300	• ㈜인성정보	02-3400-7000
	• 한국아이비엠㈜	02-3781-7800	• ㈜콤텍 시스템	02-3289-0114	• 쌍용정보통신㈜	02-2262-8114
	• 에스넷시스템㈜	02-3469-2400	• ㈜링네트	02-6675-1216	• 한국후지쯔㈜	02-3787-6000
	• 한국휴렛팩커드㈜	02-2199-0114	• ㈜LG 씨엔에스	02-6363-5000	• SK 씨앤씨㈜	02-2196-7114/8114
■ Silver 파트너	• 포스데이타㈜	031-779-2114				
■ Local 디스트리뷰터	• ㈜소프트뱅크 커머스 코리아	02-2187-0176	• ㈜아이넷뱅크	02-3400-7490	• ㈜SK 네트웍스	02-3788-3673
■ IPT 전문 파트너	• 인네트	02-3451-5300	• ㈜데이타크레프트 코리아	02-6256-7000	• 에스넷시스템㈜	02-3469-2900
	• ㈜인성정보	02-3400-7000	• ㈜크리스넷	1566-3827	• ㈜LG 씨엔에스	02-6363-5000
	• ㈜링네트	02-6675-1216				
■ IPCC 전문 파트너	• 한국아이비엠㈜	02-3781-7114	• 한국휴렛팩커드㈜	02-2199-4272	• GS 네오텍	02-2630-5280
	• ㈜인성정보	02-3400-7000	• 삼성네트웍스㈜	02-3415-6754		
■ WLAN 전문 파트너	• ㈜에어키	02-584-3717	• ㈜해창시스템	031-389-0780		
■ Security 전문 파트너	• 나래시스템	02-2190-5533	• 인포섹㈜	02-2104-5114	• 코코넛	02-6007-0133
	• UNNET Systems	02-565-7034				
■ Optical 전문 파트너	• ㈜LG 씨엔에스	02-6363-5000	• 에스넷시스템㈜	02-3469-2900	• 미리넷㈜	02-2142-2800
■ CN 전문 파트너	• ㈜메버릭시스템	02-845-4280				
■ Storage 전문 파트너	• ㈜패킷시스템즈 코리아	02-558-7170	• 매크로임팩트	02-3446-3508		