aspera
IBM® 회사

FASP 보안 모델

비즈니스 크리티컬 디지털 자산의 보안

주요 이점

- 필요한 경우 표준 오픈 소스 암호화가 대체 암호를 지원
- LDAP, Active Directory 사용자 인증
- 전송 및 저장 시 암호화를 통해 비즈니스 크리티컬 디지털 자산의 보안을 극대화
- 데이터 무결성 확인이 중간자(MITM) 공격, 재생 공격 및 UDP 서비스 거부 공격에 대한 보호를 제공

IBM® Aspera® FASP®를 포함한 모든 IBM Aspera 제품에는 표준 오픈 소스 OpenSSL 툴킷을 사용하는 데이터 전송을 위한 보안 기능이 내장되어 있습니다. 표준의 이점을 제대로 활용하기 위해 OpenSSL 암호화 라이브러리 및 표준 보안 쉘(SSH)이 수정되지 않고 사용됩니다. Aspera의 제품은 64비트 암호화를 제공하는 대중 시장 암호화 제품으로 수출하도록 미국 상무부의 승인을 받았습니다. 이 제품의 보안 모델은 세션 암호화(데이터 암호화를 위해 세션별 무작위 키를 교환하기 위한 보안 채널 수립), 전송 엔드포인트의 보안 인증, 임시 데이터 암호화 그리고 전송된 각 데이터 블록의 무결성 확인으로 이루어집니다. 전송은 지원되는 운영 체제 간에 네이티브 파일 시스템 액세스 제어 속성을 유지합니다.

세션 암호화

각 전송 작업은 표준 보안 쉘(SSH)을 사용하여 엔드포인트 간에 암호화된 보안 세션을 설정하는 것으로 시작합니다. SSH는 세션 암호화를 위한 기본 비대칭 암호 옵션인 3DES(128비트)를 사용하여 호출됩니다. SSH는 세션 암호화를 위한 다른 암호(예: 128비트 AES, Blowfish, CAST128, Arcfour, 192비트 AES 또는 256비트 AES)도 지원하며, 피어 SSH 서버에서 지원되는 경우 Aspera Scp의 명령행 호출에서 이러한 대체 암호를 요청할 수도 있습니다. 세션 암호화 키를 협상하는 데 사용되는 특정 알고리즘은 SSHv-2 또는 SSHv-1 중에서 무엇이 사용되는지에 따라 결정됩니다. SSH-v2는 Linux, Solaris 및 Mac OS X에 내장된 SSHD 서비스를 위한 기본값이고, MS Windows용 Aspera 배포와 함께 포함됩니다.

IBM

하지만 Aspera Scp는 SSH-v1과 함께 명령행 옵션으로 실행될 수 있고 또한 SSH의 다른 상용 구현 제품과 함께 작동합니다. SSH-v2는 Diffie-Hellman 키 계약을 사용하여 세션 암호화 키를 협상합니다. SSH-v1에서는 각 호스트가 호스트별 RSA 키(대개 1024비트)를 가지며 SSH 디먼이 시작될 때마다 새로운 서버 RSA 키(대개 768비트)를 동적으로 생성합니다. 이 키는 이미 사용된 경우 일반적으로 매시간 재생성되고, 디스크에 저장되지 않습니다. SSH 클라이언트가 연결하면 디먼이 공용 호스트와 서버 키를 사용하여 응답하고, 클라이언트와 서버가 세션 암호화 키를 협상합니다.

인증

보안 세션 채널이 설정되면 전송 엔드포인트가 SSH의 보안 인증 메커니즘(대화형 암호 또는 공개 키) 중 하나를 사용하여 인증을 수행합니다. 공개 키 인증의 경우 개인 키가 보안된 개인 암호구를 사용하여 암호화되고 디스크에 저장되며, RSA만(SSH-v1) 또는 RSA/DSA(SSH-v2) 공개 키 교환을 사용하여 인증이 수행됩니다. Aspera Scp의 Windows 버전에는 DSA 및 RSA 키의 생성을 위해 ssh-keygen 프로그램이 함께 배포됩니다. 기본 키 길이는 1024비트지만 사용자가 더 긴 키 길이를 요청할 수도 있습니다.

데이터 암호화

SSH 인증이 완료되면 FASP 전송 세션이 세 방향 핸드셰이크를 수행하고, 이때 원격 엔드포인트가 데이터 암호화를 위한 무작위 AES 128비트 세션별 키, 그리고 MD5 체크섬 계산을 위한 무작위 128비트 키를 생성하여 이러한 키를 보안 SSH 채널을 통해 이니시에이터로 전송합니다. 각 FASP 전송 세션에서 새로운 암호화 및 MAC 키가 생성되고, 이러한 키는 디스크에 저장되지 않습니다.

FASP는 128비트 AES 암호화를 사용하며, 이 경우 각 블록마다 고유한 비밀 난스(nonce) 또는 "초기화 벡터"와 함께 일반 CFB(Cipher Feedback, 암호 피드백) 모드를 사용하여 전송 기간 동안 키가 다시 초기화됩니다. CFB는 장시간 실행되는 전송 기간 동안 암호화된 데이터의 샘플링을 기반으로 모든 일반 공격으로부터 보호를 제공합니다.

FASP 소스 코드는 128비트 AES와 함께 암호에 대한 지원을 포함하며, AES 192 같은 다른 OpenSSL 암호를 사용하여 확장할 수 있습니다. 이때 FASP는 명령행 또는 최종 사용자가 AES 128 이외의 암호를 선택할 수 있는 GUI 옵션을 표시하지 않지만, 암호 코드가 모듈식이므로 필요하면 그렇게 할 수도 있습니다.

데이터 무결성 확인

네트워크상의 전송 이전에 모든 암호화된 데이터그램에 MD5 암호화 해시 함수(128비트)가 적용됩니다. 결과 메시지 요약이 보안 데이터그램에 추가되고 데이터 무결성을 위해(중간자 공격, 재생 공격, UDP 서비스 거부 공격을 방지하기 위해) 수신자 측에서 확인됩니다.

방화벽 고려 사항

Aspera 서버는 구성 가능한 하나의 TCP 포트(기본값은 22, 33001이 종종 사용됨)에서 하나의 SSH 서버를 실행합니다. 서버 측 방화벽은 이 하나의 TCP 포트가 Aspera 서버에 도달하도록 허용해야 합니다. UDP 포트에 실행되는 서버는 없습니다. 전송이 Aspera 클라이언트에 의해 시작된 경우, 지정된 TCP 포트의 SSH 서버에 대한 SSH 세션이 열리고 데이터가 전송될 UDP 포트(기본값 33001)가 협상됩니다. UDP 세션이 시작되도록 허용하려면 Aspera 서버 측의 방화벽에서 포트 UDP 33001이 Aspera 서버에 도달하도록 허용해야 합니다.

동시 전송 고려 사항

Aspera 서버에서 여러 개의 동시 클라이언트와 동시 전송이 이루어지는 경우:

- UNIX에서 동일한 UDP 포트를 공유합니다.
- Windows에서 일정 범위의 UDP 포트(예: 33001-33100)가 허용되어야 합니다. Windows 운영 체제에서 Aspera의 FASP 프로토콜이 여러 연결에 동일한 UDP 포트를 재사용하도록 허용하지 않기 때문입니다. 수신 클라이언트 연결은 범위 내에서 다음으로 사용 가능한 포트를 사용하도록 자동 증분됩니다.

Aspera 제품의 포인트 투 포인트 배포에서는 수신 연결을 수락하는 엔드포인트가 서버 역할을 하며, 따라서 방화벽에서 TCP 포트 22와 UDP 포트 33001(모두 구성 가능)이 Aspera 시스템에 액세스할 수 있게 허용해야 합니다.

클라이언트/서버 설치

서버 측 방화벽이 TCP 포트 및 UDP 포트에서 서버에 대한 인바운드 연결을 허용해야 합니다. Windows 서버에 한해, 잠재적인 동시 클라이언트 수(예: 33001에서 33020까지 20개의 동시 전송)를 처리하기에 충분할 만큼 큰 범위의 포트를 허용하십시오. 그 이유는 Windows가 UDP 포트 공유를 지원하지 않기 때문입니다. 서버 측 방화벽도 TCP 포트 및 UDP 포트(또는 Windows 서버를 위한 일정 범위의 포트)에서 서버로부터의 아웃바운드 연결을 허용해야 합니다.

클라이언트 측에서, 일반적인 사용자 및 비즈니스 방화벽은 TCP 및 UDP에서 클라이언트 컴퓨터의 직접 아웃바운드 연결을 허용합니다. 이 경우 Aspera 전송을 위한 별도의 구성이 필요하지 않습니다. 기업 방화벽이 직접 아웃바운드 연결을 허용하지 않는 경우(일반적으로 웹 브라우징에 프록시 서버를 사용), TCP 포트 및 UDP 포트에서 Aspera 클라이언트로부터의 아웃바운드 연결을 허용하십시오.

포인트 투 포인트 설치

두 대의 Aspera 컴퓨터 A와 B가 있다고 가정하면, A가 전송을 시작하고(A가 클라이언트) B는 수신 연결을 수락합니다(B가 서버). 클라이언트와 서버 지정은 전송 방향(업로드 또는 다운로드)과 관계없이 Aspera 전송을 시작하는 컴퓨터에 의해 결정됩니다.

클라이언트 측(컴퓨터 A)에서 일반적인 사용자 및 비즈니스 방화벽은 TCP 및 UDP에서 클라이언트 컴퓨터로부터의 직접 아웃바운드 연결을 허용합니다. 이 경우 Aspera 전송을 위한 구성이 필요하지 않습니다. 기업 방화벽이 직접 아웃바운드 연결을 허용하지 않는 경우(일반적으로 웹 브라우징에 프록시 서버를 사용) 다음과 같이 하십시오.

- TCP 포트 및 UDP 포트에서 Aspera 클라이언트로부터의 아웃바운드 연결을 허용
- 다음 중 하나를 허용:
  - 아웃바운드 UDP에 응답하는 인바운드 UDP 트래픽(대부분의 방화벽에서 이 경우가 기본값) 또는
  - 포트 33001에서의 인바운드 UDP 트래픽(비표준 방화벽 구성)

서버 측(컴퓨터 B)에서, TCP 포트에서 A로부터의 인바운드 연결을 허용하고 UDP 포트에서 B로의 인바운드 및 아웃바운드 UDP 연결을 허용하십시오.

A와 B가 클라이언트 및 서버 역할을 모두 수행하는 경우, 컴퓨터의 방화벽이 TCP 포트에서 피어에 대한/피어로부터의 아웃바운드 및 인바운드 연결을 허용하고, UDP 포트에서 피어에 대한/피어로부터의 아웃바운드 및 인바운드 UDP 연결을 허용해야 합니다.

주요 기능

- 표준 오픈 소스 OpenSSL 툴킷을 사용하는 기본 제공 전송 보안
- 표준 보안 쉘(SSH)을 사용하는 안전한 암호화된 세션
- 모든 운영 체제에서 네이티브 파일 시스템 액세스 제어를 지원하는 사용자/엔드포인트 인증
- AES-128 암호를 사용하여 전송 및 저장 시 데이터 암호화
- 전송되는 블록마다 데이터 무결성 확인

지원되는 운영 체제

- Windows 2000/XP/2003/2008, Windows Vista, Windows 7
- Mac OS 버전 10.4 이상
- Linux
- Solaris
- Isilon OneFS

방화벽 구성 요약

- Aspera는 세션 초기화 및 제어를 위해 하나의 TCP 포트를 사용하고 데이터 전송을 위해 하나의 UDP 포트를 사용합니다.
- Windows는 여러 연결에 단일 포트를 사용하도록 허용하지 않으므로 Windows에서 동시 전송을 하려면 여러 개의 UPD 포트가 필요합니다.

IBM 회사인 Aspera 정보

IBM 회사인 Aspera는 전 세계의 데이터를 파일 크기, 전송 거리 및 네트워크 상태에 관계없이 최고 속도로 이동하는 차세대 전송 기술의 개발자입니다. 특허 받은, Emmy® 상을 수상한 FASP® 프로토콜에 기반한 Aspera 소프트웨어는 기존 인프라를 완벽하게 활용하여 가장 빠르고 가장 예측 가능성이 우수한 파일 전송 환경을 제공합니다. Aspera의 핵심 기술은 대역폭에 대한 전례 없는 수준의 제어, 완벽한 보안 및 손상되지 않는 신뢰성을 제공합니다. 6개 대륙에서 다양한 업계의 기업들이 디지털 자산의 비즈니스 크리티컬 전송에 Aspera 소프트웨어를 사용합니다.

추가 정보

IBM Aspera 솔루션에 대한 추가 정보를 확인하려면 ibm.com/software/aspera를 방문하거나 Twitter에서 @asperasoft를 팔로우하십시오.

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
2015년 2월

재활용하십시오

ZZD03289-KRKO-01