(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년11월23일
(11) 등록번호 10-1086576
(24) 등록일자 2011년11월17일

(51) Int. Cl.
H04L 12/28 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2004-0049661
(22) 출원일자 2004년06월29일
심사청구일자 2009년06월25일
(65) 공개번호 10-2005-0002628
(43) 공개일자 2005년01월07일
(30) 우선권주장
10/608,334 2003년06월30일 미국(US)
(56) 선행기술조사문헌
US05010572 A1
US06845452 B1
US20020078371 A1
전체 청구항 수 : 총 15 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
베자라노,다리오바잔
미국 98074 워싱턴주 삼마미쉬 240번 애비뉴 사우스이스트 558
(74) 대리인
제일특허법인

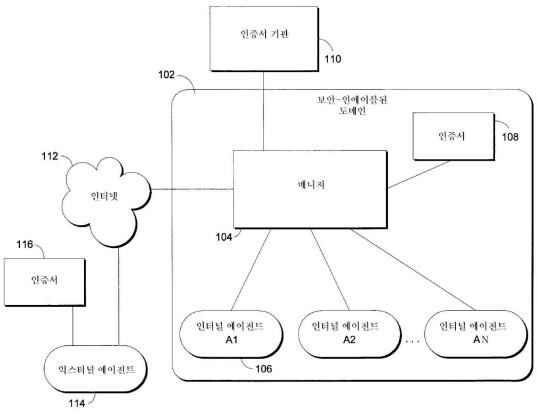
심사관 : 김선종

(54) 보안 프로토콜의 자동 협상 시스템 및 방법

(57) 요 약

프로토콜 협상 플랫폼에 의해 보안-인에이블된 도메인 외측에 존재하는 컴퓨터 또는 기타 노드가 상기한 도메인 내의 서버 또는 기타 노드와 지원가능한 보안 프로토콜을 협상할 수 있게 된다. Active Directory™, 커베로스(Kerberos) 및 기타 보안 네트워크 기술에 의해 도메인 내의 에이전트 또는 기타 노드들이 디폴트 프로토콜, 키, 인증서 또는 기타 인증 기법을 이용하여 서로 안전하게 통신할 수 있게 된다. 종래의 익스터널 에이전트는 상기한 도메인에 투명한(transparent) 방식으로 진입할 수 있는 방법이 없었으며, 상기한 도메인 경계에서 이용하기 위한 프로토콜을 수동으로 선택해야 했다. 본 발명에서는 익스터널 에이전트 또는 인터널 에이전트 어느 것이나 상기한 도메인 경계에서의 안전한 세션 확립을 위한 시도를 개시하여, 수신측 머신에 한 세트의 지원가능한 프로토콜을 포함하는 요청을 전송할 수 있다. 그러면 협상 엔진이 해당 세션의 시작 또는 끝에서 상기한 에이전트, 노드 또는 머신들에서의 이용가능한 프로토콜을 비교하여 호환가능한 프로토콜이 발견된 경우 선택하게 된다. 인터널 에이전트 및 익스터널 에이전트는 마찬가지로 키, 인증서 또는 기타 메커니즘을 이용하여 서로 인증할 수 있다.

대 표 도



특허청구의 범위

청구항 1

보안 프로토콜(security protocol)의 자동 협상(negotiate) 방법으로서, 협상 엔진에 의해,

제1 프로토콜 세트를 갖는 인터널 노드(internal node)와 제2 프로토콜 세트를 갖는 익스터널 노드(external node) 사이의 안전 접속을 확립하기 위한 보안 허가 요청(security authorization request)을 수신하는 단계 - 상기 인터널 노드는 복수의 노드들에 대한 보안 정보를 유지하는 중앙화된 분산 디렉토리(centralized distributed directory)를 포함하는 보안-인에이블된 도메인(security-enabled domain) 내에 있음 -;

상기 인터널 노드에 연관된 상기 제1 프로토콜 세트를 상기 익스터널 노드에 연관된 상기 제2 프로토콜 세트에 비교하는 단계;

상기 인터널 노드와 상기 익스터널 노드가 공통으로 2 이상의 보안 프로토콜을 포함한다는 것을 결정하는 단계;

상기 2 이상의 보안 프로토콜과 연관된 전송 속도, 및 하나 이상의 암호 키의 비트 깊이(bit depth)에 기초하여, 상기 2 이상의 보안 프로토콜 중에서 선호하는 프로토콜을 선택하는 단계 - 상기 전송 속도는 상기 2 이상의 보안 프로토콜을 이용하여 네트워크 데이터가 전송될 수 있는 속도를 나타내고, 상기 하나 이상의 암호 키의 비트 깊이는 상기 하나 이상의 암호 키를 구성하는 비트들의 수를 포함함 -; 및

상기 선호하는 프로토콜에 기초하여 상기 인터널 노드와 상기 익스터널 노드 사이의 안전 접속을 자동으로 확립하는 단계

를 포함하는, 보안 프로토콜 자동 협상 방법.

청구항 2

제1항에 있어서,

상기 익스터널 노드는 컴퓨터와 네트워크-인에이블된 무선 디바이스 중 적어도 하나를 포함하는, 보안 프로토콜 자동 협상 방법.

청구항 3

제1항에 있어서,

상기 인터널 노드는 클라이언트 컴퓨터와 서버 중 적어도 하나를 포함하는, 보안 프로토콜 자동 협상 방법.

청구항 4

제1항에 있어서,

상기 보안 허가 요청은 상기 익스터널 노드에 의해 발생되고,

선택되는 프로토콜은 전송 속도 및 키의 비트 깊이를 포함하는 기준 세트 중 적어도 하나에 기초하여 결정되는, 보안 프로토콜 자동 협상 방법.

청구항 5

제1항에 있어서,

상기 보안 허가 요청은 상기 인터널 노드에 의해 발생되고,

상기 보안 허가 요청을 수신하는 단계는 상기 익스터널 노드에 의해 실행되는, 보안 프로토콜 자동 협상 방법.

청구항 6

제1항에 있어서,

매칭하는 프로토콜이 두개 이상 발견된 경우, 상기 협상 엔진에 의해 상기 안전 접속을 확립하는 데에 사용하기 위한 프로토콜을 선택하는 단계를 더 포함하는, 보안 프로토콜 자동 협상 방법.

청구항 7

제1항에 있어서,

상기 협상 엔진에 의해, 상기 인터널 노드와 상기 익스터널 노드 중 적어도 하나를 인증하는 단계를 더 포함하는, 보안 프로토콜 자동 협상 방법.

청구항 8

보안 프로토콜의 자동 협상 시스템으로서,

노드들의 분산 디렉토리 내에 포함되는 인터널 노드 - 상기 인터널 노드는 상기 인터널 노드에 의해 지원되는 하나 이상의 보안 프로토콜을 포함하는 제1 프로토콜 세트를 저장하도록 구성됨 -; 및

협상 엔진

을 포함하고, 상기 협상 엔진은

(1) 상기 제1 프로토콜 세트를 갖는 인터널 노드와, 보안-인에이블된 도메인의 외부에 있는 익스터널 노드 사이의 안전 접속을 확립하기 위한 보안 허가 요청을 수신하고 - 상기 익스터널 노드는 상기 익스터널 노드에 의해 지원되는 보안 프로토콜을 포함하는 제2 프로토콜 세트를 저장하도록 구성됨 -,

(2) 상기 인터널 노드에 연관된 상기 제1 프로토콜 세트를 상기 익스터널 노드에 연관된 상기 제2 프로토콜 세트에 비교하고,

(3) 상기 제1 프로토콜 세트와 상기 제2 프로토콜 세트가 공통으로 2 이상의 보안 프로토콜을 포함한다는 것을 결정하고,

(4) 상기 2 이상의 보안 프로토콜에 연관된 전송 속도와, 하나 이상의 암호 키의 비트 깊이 중 적어도 하나에 기초하여, 상기 2 이상의 보안 프로토콜 중에서 선호하는 프로토콜을 선택하고 - a) 상기 전송 속도는 상기 2 이상의 보안 프로토콜을 이용하여 네트워크 데이터가 전송될 수 있는 속도를 포함하고, (b) 상기 하나 이상의 암호 키의 비트 깊이는 상기 하나 이상의 암호 키를 구성하는 비트들의 수를 포함함 -,

(5) 상기 선호하는 프로토콜에 기초하여 상기 인터널 노드와 상기 익스터널 노드 사이의 안전 접속을 자동으로 확립하도록 구성된, 보안 프로토콜 자동 협상 시스템.

청구항 9

제8항에 있어서,

상기 익스터널 노드는 컴퓨터와 네트워크-인에이블된 무선 디바이스 중 적어도 하나를 포함하는, 보안 프로토콜 자동 협상 시스템.

청구항 10

제8항에 있어서,

상기 선택된 프로토콜은 전송 속도 및 키의 비트 깊이를 포함하는 기준 세트 중 적어도 하나의 구성원에 기초하여 결정되는, 보안 프로토콜 자동 협상 시스템.

청구항 11

제8항에 있어서,

상기 협상 엔진은 상기 익스터널 노드와 상기 인터널 노드 사이의 세션이 완료된 경우 상기 안전 접속을 종료하는, 보안 프로토콜 자동 협상 시스템.

청구항 12

제8항에 있어서,

상기 협상 엔진은 상기 제1 프로토콜 세트와 상기 제2 프로토콜 세트 사이에 매칭이 발견되지 않은 경우 접속 프로세싱을 종료하는, 보안 프로토콜 자동 협상 시스템.

청구항 13

제8항에 있어서,

상기 협상 엔진은 매칭하는 프로토콜이 두개 이상 발견된 경우 상기 안전 접속을 확립하는 데에 사용하기 위한 프로토콜을 선택하는, 보안 프로토콜 자동 협상 시스템.

청구항 14

제8항에 있어서,

상기 인터널 노드와 상기 익스터널 노드 중 적어도 하나는 다른 하나를 인증하는, 보안 프로토콜 자동 협상 시스템.

청구항 15

제1항 내지 제7항 중 어느 한 항의 방법을 수행하기 위한 컴퓨터 실행가능 명령어를 포함하는, 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

청구항 59

삭제

청구항 60

삭제

청구항 61

삭제

청구항 62

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0014] 본 발명은 네트워크 컴퓨팅 기술에 관한 것으로, 특히 보안-인에이블된 도메인과 하나 이상의 익스터널 노드 사이의 보안 프로토콜의 자동 협상에 관한 것이다.

[0015] 네트워킹 기술의 발전으로 네트워크 관리자 등은 네트워크 및 기타 설비(installation)에 대한 보안 컨트롤을 보다 정교하게 유지할 수 있게 되었다. 예를 들어, Microsoft Windows™NT 2000 및 관련 제품은 관리자가 Active Directory™(AD) 구조를 이용하여 보안-인에이블된 네트워크 도메인을 전개(deploy)할 수 있도록 한다. 마찬가지로 공지의 커베로스(Kerberos) 네트워크 표준도 네트워크 내의 노드들이 키/인증 플랫폼을 이용하여 서로 인증할 수 있도록 한다. 이러한 오프레이팅 기술을 이용함으로써, 네트워크 관리자는 네트워크 서버로부터 예를 들어 규칙들, 애플리케이션, 패치, 드라이브 및 기타 자원들을, 안전한 방식으로 개별 워크스테이션 또는 기타 클라이언트에 대해 일률적인 설치를 위해 푸시(push)할 수 있다. 상기한 보안-인에이블된 도메인 내의 모든 머신들은 이들 및 기타 타입의 데이터의 전송을 투명(transparent)한 방식으로 식별 및 인증할 수 있다.

발명이 이루고자 하는 기술적 과제

[0016] 그러나, 워크스테이션에 대해 규칙, 애플리케이션 또는 기타 자원을 전달하는 것은 노드가 상기한 보안-인에이블된 도메인 외측에 존재하는 경우에는 훨씬 어려워진다. 예를 들어, 한 회사 내의 LAN 상에 수개의 컴퓨터가 존재하는 한편, Active Directory™ 또는 기타 보안-인에이블된 도메인에 속하지 않는 원격지 내의 컴퓨터와도 상호작용하는 경우가 있을 수 있다. 상기한 도메인에 대해 인터널인 머신과 그 외측의 머신 사이의 접속 확립에는 상호 지원되는 보안 프로토콜에 대한 합의가 있어야 하므로, 보안 도메인의 경계에서 통신하는 것은 보다 복잡하게 된다.

[0017] 따라서, 시스템 관리자 등은 세션이 시작되기 전에 인터널 머신과 익스터널 머신 사이에 호환되는 프로토콜을 식별함으로써 익스터널 에이전트 또는 노드의 보안-인에이블된 도메인으로의 진입(entry)을 구성하기 위해 시도해야만 한다. 예를 들어, 익스터널 에이전트는 TLS(transport layer security) 프로토콜, 커베로스-기반 프로토콜, SSL(secure socket layer) 또는 기타 프로토콜을 이용하여 상기한 보안-인에이블된 도메인 내의 관리 서버와 통신하도록 구성될 수 있다. 상기한 머신은 나아가 그 프로토콜, 즉 디폴트 프로토콜 내에 프로토콜 장애(failure)를 표시하고 상기한 익스터널 노드 또는 에이전트에 대해 프로토콜의 스위칭을 요청하거나 또는 다른 응답을 할 수도 있다. 따라서, 보안, 트랜스퍼 및 기타 프로토콜의 수동 세팅 또는 조정이 필요하며, 이 프로세스는 많은 시간이 소요될 뿐만 아니라 에러를 유발할 수 있다. 그 외에도 다른 문제가 존재할 수 있다.

발명의 구성 및 작용

[0018] 본 발명은 전술한 종래기술의 문제점을 해결한 것으로, 일 태양에 따르면, 관리자의 개입을 필요로 하지 않고 자동화된 방식으로, 익스터널 에이전트 또는 노드와의 안전한 통신이 확립되고 식별 인증될 수 있도록 한 보안 프로토콜의 자동 협상 시스템 및 방법이 제공된다. 본 발명의 일 태양에 따르면, 보안-인에이블된 도메인 내의

네트워크 매니저 또는 기타 에이전트 또는 노드가 익스터널 에이전트 또는 노드와의 안전한 접속을 확립하기 위한 시도를 개시할 수 있다. 상기한 요청은 상기한 매니저가 이용가능한 한 세트의 보안 프로토콜을 나타내는 데이터 필드를 포함하고 있다. 익스터널 에이전트는 상기한 요청을 수신하고 상기한 인터널 에이전트 또는 매니저가 이용가능한 프로토콜을 상기한 익스터널 에이전트에 의해 지원되는 한 세트의 프로토콜과 비교한다. 이용가능한 프로토콜들 사이에 매칭이 발견되면, 선택된 프로토콜에 기초하여 통신이 진행되게 된다. 본 실시예에서, 상기한 각각의 익스터널 에이전트 및 인터널 에이전트는 키, 인증서 또는 기타 인증 메커니즘을 통해 서로 인증할 수 있다.

[0019] <실시예>

[0020] 도 1은 본 발명의 실시예에 따른 프로토콜 협상 플랫폼 및 방법이 수행될 수 있는 네트워크 구조를 예시한 것이다. 도시된 바와 같이, 예시된 실시예에서는, 한 세트의 클라이언트, 서버, 에이전트 또는 기타 노드 또는 머신들이 보안-인에이블된 도메인(102)에서 동작한다. 보안-인에이블된 도메인은 본 실시예에서는 예를 들어, Microsoft Windows™ Active Directory™, 커베로스(Kerberos) 또는 기타 인증서-기반 또는 키-기반 도메인, 또는 기타 폐쇄 또는 안전 분산 디렉토리 또는 기타 환경이거나 또는 이들을 포함할 수 있다. 상기한 보안-인에이블된 도메인 내에는 예시를 위해 인터널 매니저(104)가 존재하며, 이것은 본 실시예에서 한 세트의 인터널 에이전트(106)(A1, A2, ..., AN으로 도시됨; N은 임의의 수) 뿐만 아니라 서버 또는 기타 노드이거나 이들을 포함할 수 있다.

[0021] 본 실시예에서 상기한 세트의 인터널 에이전트(106)는 추가의 서버, 워크스테이션 또는 기타 클라이언트, 또는 상기한 보안-인에이블된 도메인(102) 내에서 동작하며 상기한 인터널 매니저(104)와 통신하는 기타 인터널 에이전트 또는 노드로 구성되거나 이들을 포함할 수 있다. 본 실시예에서 상기한 인터널 매니저(104)는 상기한 세트의 인터널 에이전트(106)에 대하여 전송 또는 "푸싱" 네트워크 규칙 또는 기타 데이터와 같은 네트워크 관리 기능을 스케줄링 또는 수행하며, 상기한 기타 데이터로는 스토리지(예컨대, RAID 정책, 장애(failover) 평가기준, 메모리 한계), 대역폭 이용에 관한 동작 가이드라인 또는 기타의 규칙 또는 데이터가 있다. 이들 또는 기타 타입의 데이터를 통신하는 경우, 상기한 인터널 매니저(104) 및 상기한 세트의 인터널 에이전트(106)는 보안-인에이블된 도메인의 보안 자원을 이용하여 네트워크의 완전성(integrity) 및 규칙 및 기타 데이터의 배포를 담보한다.

[0022] 본 실시예에서는 상기한 보안-인에이블된 도메인(102)은 예컨대 인증서 108과 같은 인증서를 이용하여 인증 서비스를 제공할 수 있으며, 상기한 인증서는 X.509 또는 기타 표준 또는 포맷에 따라서 구성된 인증서이거나 또는 이를 포함할 수 있다. 키 또는 기타의 메커니즘이 마찬가지로 사용될 수도 있다. 도시된 바와 같이, 인증서(108)는 인터널 매니저(104)에 대한 인증 데이터와 연관되어 있거나 또는 이를 제공할 수도 있다. 상기한 세트의 인터널 에이전트(106) 중 어느 하나는 인증서(108)를 검증(verification)을 위해 인증서 기관(110)에 통신함으로써 인터널 매니저(104)로부터 수신한 규칙, 명령 또는 기타 데이터를 인증할 수 있다. 인증서 기관(110)은 그 자신이 보안-인에이블된 도메인(102)의 내부에 위치하거나 또는 도시된 바와 같이 상기한 보안-인에이블된 도메인(102)의 외측에 위치할 수도 있다.

[0023] 본 실시예에서, 인증서 기관(110)은 인증서(108) 또는 기타 인증 메커니즘을 판독 및 복호하여 그 결과를 상기한 세트의 인터널 에이전트(106) 또는 다른 노드들에 대해 리턴하도록 구성된 서버 또는 기타 노드이거나 또는 이들을 포함할 수 있다. 상기한 세트의 인터널 에이전트(106) 내의 각 노드들은 마찬가지로 상기한 보안-인에이블된 도메인(102)과 호환되는 인증서, 키 또는 기타 인증 데이터와 연관되어 있을 수 있다. 상기한 인터널 에이전트(106) 내의 노드들은 마찬가지로 인증서 또는 기타 메커니즘을 이용하여 서로 통신하여 상호 인증할 수도 있다.

[0024] 도 1에 도시된 실시예에서, 익스터널 에이전트(114)는 마찬가지로 통신 네트워크(112)를 통해 인터널 매니저(104)와 통신하도록 구성될 수도 있다. 상기한 익스터널 에이전트(114)도 서버, 워크스테이션 또는 기타 노드 또는 자원이거나 또는 이들을 포함할 수 있다. 또한, 상기한 익스터널 에이전트(114)는 마찬가지로 인증을 위해 상기한 익스터널 에이전트(114)를 식별하는 인증서(116)와 연관되어 있을 수도 있다. 본 실시예에서, 익스터널 에이전트(114)가 인터널 매니저(104) 또는 기타 인터널 노드와 통신을 수행할 수 있는 통신 네트워크(112)로는, 예를 들어 인터넷, 인트라넷, LAN, WAN, MAN(metropolitan area network), SAN, 프레임 릴레이 접속, AIN(Advanced Intelligent Network) 접속, SONET(synchronous optical network) 접속, 디지털 T1,T3,E1,E3 라인, DDS(Digital Data Service) 접속, ATM 접속, FDDI(Fiber Distributed Data Interface), CDDI(Copper Distributed Data Interface) 기타 유선, 무선 또는 광학 접속 중 어느 하나 이상이거나, 이들을 포함하거나 이

들과 인터페이스할 수 있다. 익스터널 에이전트(114)는 본 실시예에서 워크스테이션, 서버, 무선 네트워크-인에이블된 장치, 또는 네트워크 통신용으로 구성된 기타 노드, 에이전트 또는 플랫폼이거나 또는 이들을 포함할 수 있다.

[0025] 종래의 크로스-도메인 통신 구현과 달리, 본 발명에 따르면 상기한 익스터널 에이전트(114)는 인터널 매니저(104)와 컨택을 개시하여 상호 호환되는 프로토콜에 기초하여 자동 또는 투명한 방식으로 호환 프로토콜을 서로 선택함으로써 안전 접속을 확립할 수 있다. 도 2에 예시된 바와 같이, 익스터널 에이전트(114)에서 실행되는 익스터널 애플리케이션(130)은 익스터널 협상 엔진(126)을 통해 인터널 매니저와 컨택을 개시할 수 있다. 익스터널 애플리케이션(130)은 데이터 백업 스케줄러, 방화벽, 바이러스 보호 또는 기타 애플리케이션 등과 같은 시스템 유틸리티, 생산성(productivity) 또는 기타 애플리케이션이거나 이들을 포함할 수 있다. 익스터널 애플리케이션(130)은 예를 들어 각종의 태스크를 수행하여 인터널 매니저(104)와 상기한 통신을 수행하기 위한 사용자 프로파일, 업데이트 또는 기타 데이터를 필요로 할 수 있다.

[0026] 익스터널 협상 엔진(126)은 익스터널 애플리케이션(130)에 의해 요청된 통신을 처리 및 관리하여 상기한 인터널 매니저(104)에 대한 상호 호환가능한 통신 링크를 보안-인에이블된 도메인(102)에 확립할 수 있다. 본 실시예에서는 도시된 바와 같이 상기한 익스터널 협상 엔진(126)은 협상 모듈(1180을 개시 및 관리할 수 있으며, 이것은 공지된 SPNEGO(Simple and Protected GSS-API Negotiation) 프로토콜의 구현예이다. 다른 프로토콜이 사용될 수도 있다. 본 실시예에서, 상기한 협상 모듈(118)은 익스터널 에이전트(114)의 오퍼레이팅 시스템인 예를 들어 애플리케이션 프로그램 인터페이스(API) 또는 기타 메커니즘을 통해 액세스, 개시 또는 발생될 수 있다.

[0027] 익스터널 협상 엔진(126)은 마찬가지로 프로토콜 협상 프로세스를 실행하기 위해 익스터널 에이전트(114)에 의해 채용될 수 있는 기타 채널 또는 메시지-기반 채널을 지시하는 익스터널 트랜스포트 지정자(120)(specifier)를 포함 또는 발생시킬 수 있다. 예를 들어, 본 실시예에서 익스터널 트랜스포트 지정자(120)는 Microsoft .NET 아키텍처의 일부분으로서 SSPI(Security Support Provider Interface) 프로토콜을 지정하여, 익스터널 애플리케이션(130) 또는 기타 소프트웨어 또는 모듈들이 예컨대 DLL(dynamic link libraries) 또는 표준 암호(cryptographic) 또는 기타 인코딩 방식을 지원하는 기타 자원에 액세스할 수 있도록 할 수 있다. 익스터널 트랜스포트 지정자(120) 내에 다른 프로토콜이 사용 또는 지정될 수도 있다. 익스터널 협상 엔진(126)은 도 2에 도시된 바와 같이 결과적으로 상기한 데이터 또는 기타 데이터를 지시하는 데이터그램(datagram)을 인터널 매니저(104)에 접속된 인터널 협상 엔진(128)에 통신할 수 있다.

[0028] 인터널 협상 엔진(128)은 마찬가지로 협상 모듈(122) 및 인터널 트랜스포트 지정자(124)를 포함하거나 또는 이들을 인터페이스할 수 있다. 인터널 협상 엔진(128)은 또한 인터널 매니저(104)에서 실행되거나 또는 인터널 매니저(104)에 의해 액세스된 인터널 애플리케이션(132)과 통신할 수 있다. 예를 들어, 인터널 애플리케이션(132)은 시스템 관리, 생산성 또는 기타 애플리케이션이거나 또는 이를 포함할 수 있다. 상기한 인터널 협상 엔진(128)은 인터널 매니저(104)와의 통신 확립 요청을 수신하면, 예를 들어 상기한 SSPI 프로토콜을 이용하여 채널 통신을 확인(confirm)함으로써 인터널 트랜스포트 지정자(124)를 통해 익스터널 에이전트(114)와 메시지-기반 또는 기타 채널을 확립할 수 있다.

[0029] 익스터널 에이전트(114)와 인터널 매니저104) 사이에 예비(preliminary) 채널이 확립된 상태에서, 상기한 익스터널 협상 엔진(126) 및 익스터널 협상 엔진(128)은 프로토콜 협상 및 감축(reduction)을 개시할 수 있다. 본 실시예에서, 익스터널 에이전트(114)는 도 3에 도시된 익스터널 프로토콜 테이블(134)을 익스터널 매니저(104)에 전송한다. 상기한 익스터널 프로토콜 테이블(134)은 익스터널 에이전트(114)가 구성된 프로토콜을 지정할 수 있다. 상기한 인터널 매니저(104)가 익스터널 프로토콜 테이블(134)을 수신하면, 상기한 테이블(134)은 인터널 매니저(104)에서 이용가능한 한 세트의 보안 프로토콜을 나타내는 인터널 프로토콜 테이블(136)과 비교된다. 상기한 익스터널 프로토콜 테이블(134)과 인터널 프로토콜 테이블(136) 중 어느 하나는 예를 들어 TLS(transport layer security), SSL(secure socket layer), 커베로스(Kerberos), IPSec(secure IP) 또는 기타 이용가능한 프로토콜 또는 표준을 나타내는 필드를 포함하고 있다. 상기한 인터널 매니저(104)에 접속된 협상 엔진(128)은 도 3에 도시된 바와 같이 익스터널 에이전트(114) 및 인터널 매니저(104)에 의해 상호 지원되는 하나 이상의 프로토콜을 식별하게 된다.

[0030] 본 실시예에서, 협상 엔진(128)은 마찬가지로 프로토콜 비교를 위해 익스터널 에이전트(114)에 접속된 협상 엔진(126)에 인터널 프로토콜 테이블(136)을 통신한다. 협상 엔진(126) 및 협상 엔진(128)은 그 결과 보안-인에이블된 도메인에서 안전 통신을 확립하기 위하여 서로 이용가능한 프로토콜의 선택을 협상한다. 예를 들어, 익스터널 에이전트(114)와 인터널 매니저(104) 양방에 단지 하나의 공통 프로토콜이 이용가능하다면, 익스터널 에

이전트(114) 및 인터널 매니저(104)는 TLS 또는 기타 프로토콜 등 해당 프로토콜을 이용하여 세션을 셋업하는데 합의할 것이다. 협상 엔진(126) 및 협상 엔진(128)이 공통 프로토콜이 발견되지 않을 것이라는데 합의한다면, 크로스-도메인 통신을 확립하기 위한 시도는 종료될 것이다. 반대로, 협상 엔진(126) 및 협상 엔진(128)이 다수의 프로토콜이 공통인 것을 확인한다면, 전송(transfer) 속도, 키의 비트 깊이(depth) 또는 기타 보안 메커니즘 등의 네트워크 평가기준 또는 기타의 팩터에 기초하여 사용할 하나의 프로토콜을 선택할 것이다.

[0031] 상호 호환되는 프로토콜을 위치시켜 두면, 익스터널 에이전트(114)와 인터널 매니저(104) 사이에는 안전 세션이 확립될 것이다. 본 실시예에서는 보안을 강화하기 위하여 익스터널 에이전트(114) 및 인터널 매니저(104)는 각각 마찬가지로 인증(authentication) 단계를 수행하여 상대방 노드의 ID, 특권(privilege) 레벨 또는 기타 보안 상세를 검증(verify)할 것이다. 도 1에 도시된 바와 같이, 이것은 인증서 또는 기타 보안 메커니즘을 이용하여 수행될 수 있다. 익스터널 에이전트(114)는 인증서(108)를 인증서 기관(110)에 통신함으로써 인터널 매니저(104)를 인증할 수 있다. 반대로, 인터널 매니저(104)는 인증서(116)를 인증서 기관(110)에 통신함으로써 익스터널 에이전트(114)를 인증할 수 있다. 기타의 보안 메커니즘이 이용될 수도 있다.

[0032] 본 실시예에서, 상기한 익스터널 에이전트(114)와 인터널 매니저(104) 사이에 교환되는 데이터의 타입 또는 콘텐트는 이들 2개 노드 사이의 상호 인증에 종속할 것이다. 예를 들어, 네트워크 관리 규칙 또는 파라미터에의 액세스는 인터널 노드 또는 익스터널 노드에 대해 예비되어 있고 단지 주어진 액세스의 특권 레벨만을 지시할 수도 있다. 기타의 인증 규칙 또는 평가기준이 이용될 수도 있다. 동작상의 보안 프로토콜이 확립되고 인증 처리가 완료된 후, 상기한 익스터널 에이전트(114)와 인터널 매니저(104)는 데이터, 애플리케이션, 규칙 또는 기타 정보를 교환하게 된다. 트래픽이 완료되면, 협상 엔진(126) 및 협상 엔진(128)은 상기한 통신 링크를 해제(release) 또는 종료(terminate)한다.

[0033] 도 4는 본 발명의 실시예에 따른 전반적인 네트워크 협상 프로세싱을 예시하고 있다. 단계 402에서 프로세싱이 개시된다. 단계 404에서, 익스터널 에이전트(114), 인터널 매니저(104) 또는 기타 클라이언트, 에이전트 또는 노드에 의해 보안-인에이블된 네트워크(102)에서의 안전 접속 확립을 위한 요청이 생성된다. 단계 406에서, 상기 안전 접속 확립 요청이 수신측 노드에 전송되며, 여기서 수신측 노드는 인터널 매니저(104), 익스터널 에이전트(114) 또는 기타의 클라이언트, 에이전트 또는 노드일 수 있으며, 상기한 요청은 전송측 노드와 호환되는 제1 프로토콜 세트를 포함하고 있다. 단계 408에서, 상기 요청이 수신측 노드에 수신된다. 단계 410에서, 인터널 매니저(104), 익스터널 에이전트(114) 또는 기타의 클라이언트, 에이전트 또는 노드일 수 있는 수신측 노드가 상기 제1 프로토콜 세트를 상기 수신측 노드의 제2 프로토콜 세트와 비교하여, 이용가능한 프로토콜들 중에서 매칭 여부를 판정한다.

[0034] 상기한 제1 프로토콜 세트와 제2 프로토콜 세트 사이에 매칭이 발견되면, 상기한 프로세싱은 단계 412로 진행하여, 하나보다 많은 매칭 프로토콜이 발견되었는지를 판정한다. 하나보다 많은 매칭 프로토콜이 발견되었다면, 단계 414로 프로세싱을 진행하여, 전송 속도, 키의 비트 깊이 또는 기타 보안 메커니즘 등의 프로토콜 평가기준 또는 기타의 팩터에 기초하여 매칭 프로토콜들 중에서 사용할 하나의 프로토콜을 선택한다. 그런 다음, 단계 416으로 프로세싱을 진행하여, 선택된 프로토콜에 기초하여 익스터널 에이전트(114)와 인터널 매니저(104) 사이에 안전 접속 또는 세션이 개시된다. 마찬가지로, 단계 412에서 단지 하나의 매칭 프로토콜이 발견된 경우에도, 단계 416으로 프로세싱을 진행하여, 안전 접속 또는 세션이 개시될 수 있다. 예를 들어, 본 실시예에서 지정된 포트들은 상기한 TCP/IP 또는 기타 통신 또는 기타 프로토콜 아래에서 개방될 것이다.

[0035] 단계 418에서, 상기한 매칭 프로토콜에 따라 핸드쉐이크 및 기타 단계를 진행함으로써 상기한 익스터널 에이전트(114)와 인터널 매니저(104) 사이에 프로토콜-특정 교환이 개시되게 된다. 단계 420에서, 상기한 익스터널 에이전트(114)와 인터널 매니저(104) 중 어느 하나 또는 양방은 [상기한 익스터널 에이전트(114)의] 대응하는 인증서(116) 또는 [상기한 인터널 매니저(104)의] 대응하는 인증서(108)를 인증서 기관(110)에 절절하게 전송함으로써 대응하는 상대방 노드를 인증할 수 있다. 본 실시예에서, 상기한 인증서 116 또는 인증서 108 또는 기타 보안 데이터는 X.509 표준 또는 기타 표준 또는 포맷에 합치하는 인증서 오브젝트이거나 이들을 포함할 수 있다. 적절한 인증이 완료되면, 단계 422로 프로세싱을 진행하여, 상기한 익스터널 에이전트(114)와 인터널 매니저(104) 사이에 안전 접속 또는 세션을 수행하게 된다. 예를 들어, 이들 2개 노드 사이에서 시스템 관리 또는 기타의 목적으로 네트워크 또는 기타 규칙이 통신될 수도 있다.

[0036] 안전 세션이 완료되면 단계 424로 프로세싱을 진행하여, 상기한 익스터널 에이전트(114)와 인터널 매니저(104) 사이의 안전 접속을 종료 또는 해제한다. 단계 426에서, 프로세싱이 종료되거나 반복 수행되어, 선행 프로세싱 포인트로 리턴하거나 또는 다른 액션을 수행할 수도 있다. 마찬가지로, 단계 410에서 매칭 프로토콜이 확인되

지 않은 것으로 판정된 경우, 단계 426으로 진행하여 프로세싱을 종료하거나 반복 수행하거나 또는 선행 프로세싱 포인트로 리턴하거나 또는 다른 액션을 수행할 수도 있다.

[0037] 전술한 설명은 예시를 위한 것일 뿐이며 본 기술분야의 전문가라면 구성 및 구현시 각종의 수정이 가능할 것이다. 예를 들어, 본 발명을 하나의 익스터널 에이전트(114)와 관련하여 설명하였지만, 복수의 익스터널 에이전트 또는 노드가 보안-인에이블된 도메인(102) 내의 인터널 매니저(104) 또는 기타 클라이언트 또는 노드와의 매칭 프로토콜 협상을 자동적으로 수행하도록 구성할 수도 있다. 마찬가지로, 인증 메커니즘에 있어서도 상기한 메커니즘이 X.509 또는 기타 표준을 이용하여 하나의 인증 엔티티(110)에 의해 지원되고 있는 것으로 설명하였지만, 다수의 인증 엔티티 또는 기타 인증 또는 허가 플랫폼이 채용될 수도 있다. 그밖에도, 하드웨어, 소프트웨어 또는 기타 자원들을 하나만 도시/설명하였지만 이들이 분산되어 있을 수도 있으며, 마찬가지로 분산되어 있는 것으로 도시/설명된 자원들이 결합되어 있을 수도 있다.

[0038] 또한, 보안-인에이블된 도메인(102)에 대해 익스터널인 일방 또는 타방의 노드 또는 에이전트와, 상기한 도메인에 대해 인터널인 노드 또는 에이전트가 보안 프로토콜의 협상을 개시하는 것으로 설명하였지만, 본 발명에 따라 구성된 임의의 노드 또는 에이전트는 상기한 도메인에 대해 익스터널 또는 인터널인지에 무관하게 프로토콜 프로세싱을 개시할 수 있다. 마찬가지로, 인터널 및 익스터널 에이전트의 어느 일방 또는 양방이 상대방 에이전트 또는 노드에 대한 인증을 개시할 수도 있다. 따라서, 본 발명의 범위는 특허청구범위에 의해서만 제한되는 것으로 이해되어야 한다.

발명의 효과

[0039] 전술한 바와 같이, 본 발명의 보안 프로토콜의 자동 협상 시스템 및 방법에 따르면, 관리자의 개입을 필요로 하지 않고 자동화된 방식으로 익스터널 에이전트 또는 노드와의 안전한 통신 확립 및 인증이 가능하게 된다.

도면의 간단한 설명

[0001] 도 1은 본 발명의 실시예가 동작될 수 있는 네트워크 구조를 예시한 도면.

[0002] 도 2는 본 발명의 실시예에 따른 인터널 노드와 익스터널 노드 사이의 협상 프로세스를 예시한 도면.

[0003] 도 3은 본 발명의 실시예에 따른 프로토콜 테이블들 사이의 비교를 예시한 도면.

[0004] 도 4는 본 발명의 실시예에 따른 전반적인 프로토콜 협상 프로세싱을 예시한 도면.

[0005] <도면의 주요 부분에 대한 부호의 설명>

[0006] 102: 보안-인에이블된 도메인

[0007] 104: 매니저

[0008] 106: 인터널 에이전트

[0009] 108: 인증서

[0010] 110: 인증서 기관

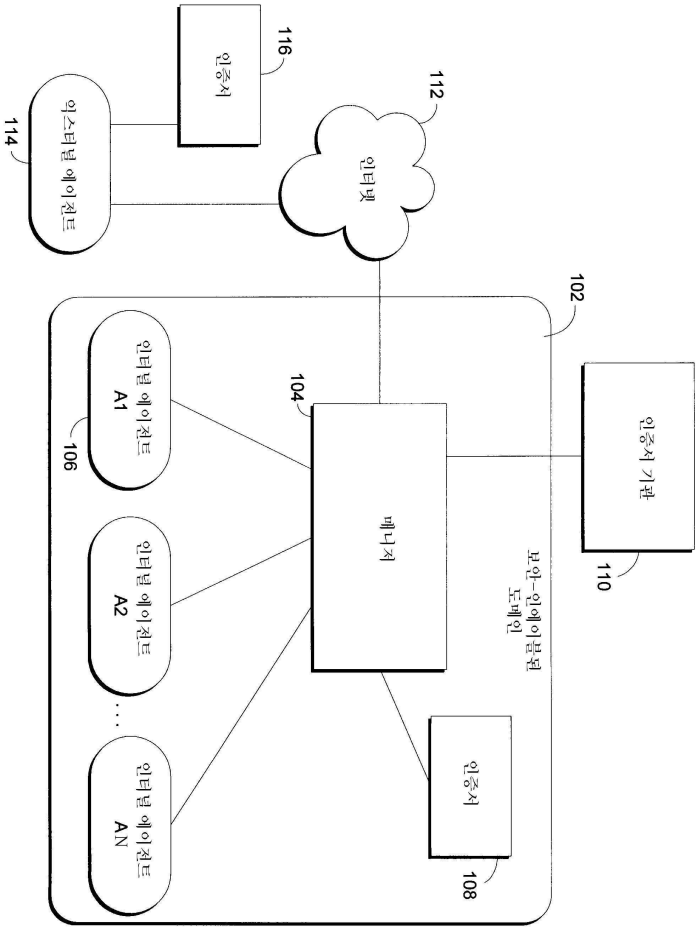
[0011] 112: 인터넷

[0012] 114: 익스터널 에이전트

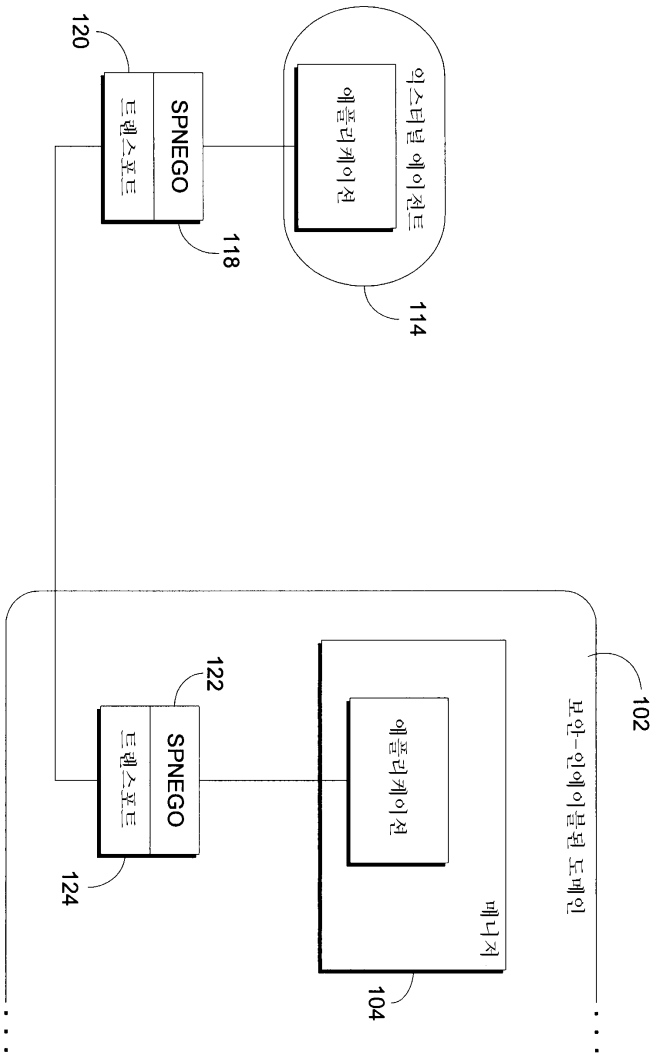
[0013] 116: 인증서

도면

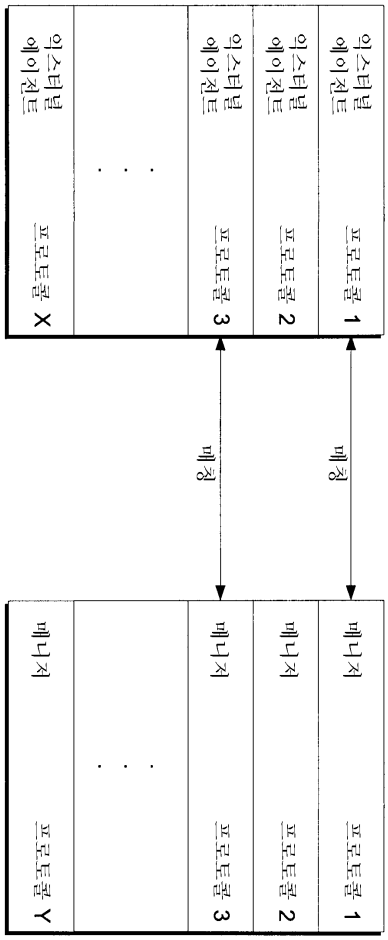
도면1


인증서
116
112
인터넷
익스터널 에이전트
114
102
인터널 에이전트
A1
106
104
매니저
인증서 기관
110
인터널 에이전트
A2
...
인터널 에이전트
AN
인증서
108
분산-인에이블러
도메인

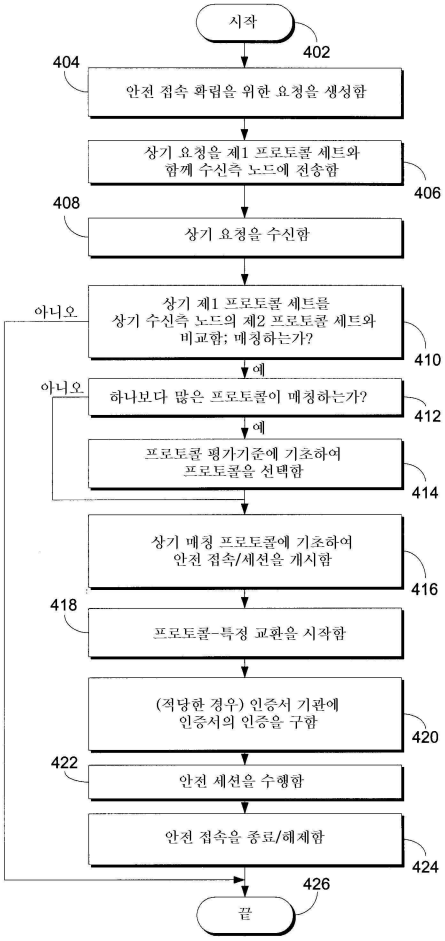
도면2


보안-인에이블드 도메인
102
매니저
104
애플리케이션
SPNEGO
트랜스포트
122
124
익스터널 에이전트
114
애플리케이션
SPNEGO
트랜스포트
118
120

도면3


익스터널 에이전트 프로토콜 1
익스터널 에이전트 프로토콜 2
익스터널 에이전트 프로토콜 3
익스터널 에이전트 프로토콜 X
매칭
매칭
메니저 프로토콜 1
메니저 프로토콜 2
메니저 프로토콜 3
메니저 프로토콜 Y

도면4


시작
402
404
안전 접속 확립을 위한 요청을 생성함
상기 요청을 제1 프로토콜 세트와 함께 수신측 노드에 전송함
406
408
상기 요청을 수신함
상기 제1 프로토콜 세트를 상기 수신측 노드의 제2 프로토콜 세트와 비교함; 매칭하는가?
410
아니오
예
하나보다 많은 프로토콜이 매칭하는가?
412
아니오
예
프로토콜 평가기준에 기초하여 프로토콜을 선택함
414
상기 매칭 프로토콜에 기초하여 안전 접속/세션을 개시함
416
418
프로토콜-특정 교환을 시작함
(적당한 경우) 인증서 기관에 인증서의 인증을 구함
420
422
안전 세션을 수행함
안전 접속을 종료/해제함
424
426
끝