(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0086659
(43) 공개일자 2020년07월17일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/12* (2006.01)
(52) CPC특허분류
H04L 63/0236 (2013.01)
H04L 61/2015 (2013.01)
(21) 출원번호 10-2020-7009850
(22) 출원일자(국제) 2018년09월11일
심사청구일자 없음
(85) 번역문제출일자 2020년04월06일
(86) 국제출원번호 PCT/US2018/050411
(87) 국제공개번호 WO 2019/055391
국제공개일자 2019년03월21일
(30) 우선권주장
15/702,355 2017년09월12일 미국(US)

(71) 출원인
시너젝스 그룹
미국 코네티컷 06830 그리니치 코브 아일랜드 드라이브 19
데일러 웨인
미국 아리조나 85249 챈들러 이스트 틱우드 플레이스 2117
팜 홀딩스, 인크.
미국 워싱턴 98513 레이시 24 번 코트 사우스이스트 9227
(72) 발명자
팜 티엔 반
미국 워싱턴 98513 레이시 24번 코트 사우스이스트 9227
(74) 대리인
리앤목특허법인

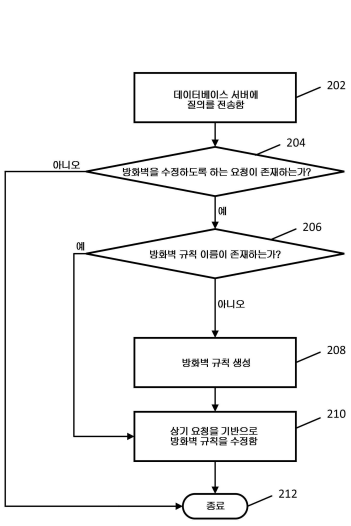
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **동적 ＩＰ 주소를 기반으로 방화벽을 수정하는 방법, 시스템 및 매체**

(57) 요 약

동적 인터넷 프로토콜(Internet Protocol; IP) 주소를 기반으로 방화벽 규칙을 수정하는 방법, 시스템 및 매체가 제공된다. 일부 실시 예들에서, 상기 방법은, 데이터베이스 서버로부터, 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 단계 - 상기 요청에는 상기 원격 컴퓨터에 대한 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -; 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 단계; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 단계;를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/0263 (2013.01)
H04L 63/08 (2013.01)
H04L 63/105 (2013.01)
H04L 63/20 (2013.01)

명 세 서

청구범위

청구항 1

동적 인터넷 프로토콜(Internet Protocol; IP) 주소를 기반으로 방화벽 규칙을 수정하는 방법으로서,

데이터베이스 서버로부터, 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 단계 - 상기 요청에는 상기 원격 컴퓨터와의 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -;

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 단계; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 단계;

를 포함하는, 방화벽 규칙의 수정 방법.

청구항 2

제1항에 있어서,

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 할지를 결정하는 단계; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙으로부터 제거하는 단계;

를 더 포함하는, 방화벽 규칙의 수정 방법.

청구항 3

제1항에 있어서,

상기 방화벽 규칙이 존재하지 않는다고 결정하는 단계; 및

상기 방화벽 규칙이 존재하지 않는다는 결정에 응답하여, 상기 방화벽 규칙을 생성하는 단계;

를 더 포함하는, 방화벽 규칙의 수정 방법.

청구항 4

제1항에 있어서,

상기 요청에는 상기 방화벽 규칙을 나타내는 방화벽 규칙 이름이 포함되는, 방화벽 규칙의 수정 방법.

청구항 5

제1항에 있어서,

상기 요청은 상기 데이터베이스 서버에 전송되는 질의에 응답하여 상기 데이터베이스 서버로부터 수신되는, 방화벽 규칙의 수정 방법.

청구항 6

동적 인터넷 프로토콜(Internet Protocol; IP) 주소를 기반으로 방화벽 규칙을 수정하는 시스템으로서,

상기 시스템은 하드웨어 프로세서를 포함하며,

상기 하드웨어 프로세서는,

데이터베이스 서버로부터, 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 동작 - 상기 요청에는 상기 원격 컴퓨터와의 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽

규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -;

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 동작; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 동작;

을 수행하도록 프로그램되는, 방화벽 규칙의 수정 시스템.

청구항 7

제6항에 있어서,

상기 하드웨어 프로세서는,

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 할지를 결정하는 동작; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙으로부터 제거하는 동작;

을 더 수행하도록 프로그램되는, 방화벽 규칙의 수정 시스템.

청구항 8

제6항에 있어서,

상기 하드웨어 프로세서는,

상기 방화벽 규칙이 존재하지 않는다고 결정하는 동작; 및

상기 방화벽 규칙이 존재하지 않는다는 결정에 응답하여, 상기 방화벽 규칙을 생성하는 동작;

을 더 수행하도록 프로그램되는, 방화벽 규칙의 수정 시스템.

청구항 9

제6항에 있어서,

상기 요청에는 상기 방화벽 규칙을 나타내는 방화벽 규칙 이름이 포함되는, 방화벽 규칙의 수정 시스템.

청구항 10

제6항에 있어서,

상기 요청은 상기 데이터베이스 서버에 전송되는 질의에 응답하여 상기 데이터베이스 서버로부터 수신되는, 방화벽 규칙의 수정 시스템.

청구항 11

프로세서에 의해 실행될 때 상기 프로세서로 하여금 동적 인터넷 프로토콜(Internet Protocol; IP) 주소를 기반으로 방화벽 규칙을 수정하는 방법을 수행하게 하는 컴퓨터 실행가능 명령어들을 포함하는 비-일시적 컴퓨터 판독가능 매체로서,

상기 방법은,

데이터베이스 서버로부터, 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 단계 - 상기 요청에는 상기 원격 컴퓨터에 대한 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -;

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 단계; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 단계;

를 포함하는, 비-일시적 컴퓨터 판독가능 매체.

청구항 12

제11항에 있어서,

상기 방법은,

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 할지를 결정하는 단계; 및

사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙으로부터 제거하는 단계;

를 더 포함하는, 비-일시적 컴퓨터 판독가능 매체.

청구항 13

제11항에 있어서,

상기 방법은,

상기 방화벽 규칙이 존재하지 않는다고 결정하는 단계; 및

상기 방화벽 규칙이 존재하지 않는다는 결정에 응답하여, 상기 방화벽 규칙을 생성하는 단계;

를 더 포함하는, 비-일시적 컴퓨터 판독가능 매체.

청구항 14

제11항에 있어서,

상기 요청에는 상기 방화벽 규칙을 나타내는 방화벽 규칙 이름이 포함되는, 비-일시적 컴퓨터 판독가능 매체.

청구항 15

제11항에 있어서,

상기 요청은 상기 데이터베이스 서버에 전송되는 질의에 응답하여 상기 데이터베이스 서버로부터 수신되는, 비-일시적 컴퓨터 판독가능 매체.

발명의 설명

기 술 분 야

[0001] 관련 출원에 대한 상호 참조

[0002] 본원은 2017년 9월 12일자로 출원된 미국 특허출원 제15/702,355호의 이점을 주장하며, 상기 미국 특허출원 전체는 이로써 인용에 의해 본원 명세서에 보완된다.

[0003] 기술분야

[0004] 개시된 주제는 동적 IP 주소를 기반으로 방화벽을 수정하는 방법, 시스템 및 매체에 관한 것이다.

배 경 기 술

[0005] 많은 사용자는 원격 컴퓨터에 대한 원격 데스크톱 접속을 확립하려고 한다. 예를 들어, 사무실에서 멀리 떨어져 있는 사용자는 공용 네트워크 접속을 통해서 랩톱 컴퓨터를 사용해 업무용 컴퓨터에 대한 원격 데스크톱 접속을 확립하려고 할 수 있다. 그러나 경우에 따라서는, 알 수 없는 주소가 원격 컴퓨터에 액세스하는 것을 방화벽이 차단하기 때문에 사용자가 원격 데스크톱 접속을 확립하지 못하도록 차단될 수 있다. 또한, 경우에 따라서는, 사용자의 IP 주소가 이러한 방화벽으로 프로그래밍될 수 있는 경우에도 사용자의 인터넷 서비스 공급자(Internet Service Provider; ISP)에 의해 IP 주소가 동적으로 할당되기 때문에 사용자 컴퓨터의 IP 주소를 알 수 없는 경우도 있다.

[0006] 따라서, 동적 IP 주소를 기반으로 방화벽을 수정하는 새로운 방법, 시스템 및 매체를 제공하는 것이 바람직하다.

발명의 내용

[0007] 동적 IP 주소를 기반으로 방화벽을 수정하는 방법, 시스템 및 매체가 제공된다. 개시된 주제의 일부 실시 예들에 의하면, 동적 IP 주소를 기반으로 방화벽을 수정하는 방법이 제공되며, 상기 방법은 데이터베이스 서버로부터 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 단계 - 상기 요청에는 상기 원격 컴퓨터와의 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -; 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 단계; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 단계;를 포함한다.

[0008] 개시된 주제의 일부 실시 예들에 의하면, 동적 IP 주소를 기반으로 방화벽을 수정하는 시스템이 제공되며, 상기 시스템은 데이터베이스 서버로부터 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 동작 - 상기 요청에는 상기 원격 컴퓨터와의 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -; 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 동작; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 동작;을 수행하도록 프로그램된 하드웨어 프로세서를 포함한다.

[0009] 개시된 주제의 일부 실시 예들에 의하면, 프로세서에 의해 실행될 때 상기 프로세서로 하여금 동적 IP 주소를 기반으로 방화벽을 수정하는 방법을 수행하게 하는 컴퓨터 실행가능 명령어들을 포함하는 비-일시적 컴퓨터 판독가능 매체가 제공된다. 상기 방법은 데이터베이스 서버로부터 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 단계 - 상기 요청에는 상기 원격 컴퓨터에 대한 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -; 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 단계; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 단계;를 포함한다.

[0010] 개시된 주제의 일부 실시 예들에 의하면, 동적 IP 주소를 기반으로 방화벽을 수정하는 시스템이 제공되며, 상기 시스템은 데이터베이스 서버로부터 원격 컴퓨터를 보호하는 방화벽의 방화벽 규칙을 수정하도록 하는 요청을 수신하는 수단 - 상기 요청에는 상기 원격 컴퓨터와의 접속을 개시하는 사용자 장치의 IP 주소가 포함되고, 상기 방화벽 규칙에는 상기 원격 컴퓨터와의 접속을 확립하도록 허용되는 장치의 IP 주소가 표시됨 -; 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 하는 지를 결정하는 수단; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 한다는 결정에 응답하여, 현재 IP 주소를 상기 방화벽 규칙에 추가하는 수단;을 포함한다.

[0011] 일부 실시 예들에서, 상기 시스템은 사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 하는 지를 결정하는 수단; 및 사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 한다는 결정에 응답하여 상기 방화벽 규칙으로부터 현재 IP 주소를 제거하는 수단을 더 포함한다.

[0012] 일부 실시 예들에서, 상기 시스템은 상기 방화벽 규칙이 존재하지 않는다고 결정하는 수단; 및 상기 방화벽 규칙이 존재하지 않는다는 결정에 응답하여 상기 방화벽 규칙을 생성하는 수단을 더 포함한다.

[0013] 일부 실시 예들에서, 상기 요청에는 상기 방화벽 규칙을 나타내는 방화벽 규칙 이름이 포함된다.

[0014] 일부 실시 예들에서, 상기 요청은 상기 데이터베이스 서버에 전송된 질의에 응답하여 상기 데이터베이스 서버로부터 수신된다.

[0015] 개시된 주제의 다양한 목적, 특징 및 이점은 이하의 도면과 연관지어 고려될 때 개시된 주제의 이하의 상세한 설명을 참조하여 더 충분히 이해될 수 있으며, 도면에서는 동일한 참조 번호가 동일한 요소를 나타낸다.

도면의 간단한 설명

[0016] 도 1은 개시된 주제의 일부 실시 예들에 따른 방화벽에 IP 주소를 추가하도록 하는 요청을 생성하는 프로세스의 일 예를 보여주는 도면이다.

도 2는 개시된 주제의 일부 실시 예들에 따른 회수된 요청을 기반으로 방화벽을 수정하는 프로세스의 일 예를 보여주는 도면이다.

도 3은 개시된 주제의 일부 실시 예들에 따른 동적 IP 주소를 기반으로 방화벽을 수정하기에 적합한 전형적인 시스템의 개략도이다.

도 4는 개시된 주제의 일부 실시 예들에 따른 도 3의 서버 및/또는 사용자 장치에서 사용될 수 있는 하드웨어의 상세한 예를 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 다양한 실시 예에 의하면, 동적 IP 주소를 기반으로 방화벽을 수정하는 메커니즘(이는 방법, 시스템 및 매체를 포함할 수 있음)이 제공된다.

[0018] 일부 실시 예들에서, 본원 명세서에 기재되어 있는 메커니즘은 방화벽의 차단되지 않은 IP 주소들의 리스트에 IP 주소를 동적으로 그리고 원격으로 추가할 수 있고 그럼으로써 예컨대, 사용자가 상기 방화벽에 의해 보호되는 원격 컴퓨터에 대한 원격 데스크톱 접속을 확립할 수 있게 한다. 일부 실시 예들에서, 사용자 장치는 동적 인터넷 프로토콜(IP) 주소를 지닐 수 있다. 이러한 일부 실시 예들에서, 상기 사용자 장치는 상기 사용자 장치에 연관된 현재 IP 주소 및 상기 원격 컴퓨터에 연관된 방화벽 규칙에 상기 IP 주소를 추가하도록 하는 요청을 포함하는 메시지를 데이터베이스 서버에 전송할 수 있다. 일부 실시 예들에서, 상기 원격 컴퓨터는 현재 IP 주소를 회수하기 위해 쿼리(query)를 데이터베이스 서버에 전송할 수 있고, 이어서 현재 IP 주소를 포함시키도록 상기 원격 컴퓨터에 연관된 방화벽 규칙을 업데이트할 수 있다.

[0019] 도 1을 참조하면, 개시된 주제의 일부 실시 예들에 따른, 사용자 장치에 연관된 IP 주소가 방화벽에 추가되도록 요청하는 프로세스(100)의 일 예가 도시되어 있다. 일부 실시 예들에서, 프로세스(100)의 블록들은 방화벽에 의해 보호되는 원격 컴퓨터에 대한 액세스(예컨대, 상기 원격 컴퓨터와의 원격 데스크톱 접속을 확립하도록 하는 액세스)를 추구하는 사용자 장치와 같은 임의의 적합한 장치에 의해 실행될 수 있다. 더 구체적으로는, 일부 실시 예들에서, 프로세스(100)의 블록들은 상기 장치상에서 실행되는 프로그램(예컨대, 웹 애플리케이션, 독립형 애플리케이션 및/또는 임의의 다른 적절한 프로그램)에 의해 실행될 수 있다.

[0020] 프로세스(100)는 프로세스(100)를 실행하는 사용자 장치를 데이터베이스 서버(예컨대, 도 3에 도시되고 도 3과 관련지어 이하에 기재되어 있는 바와 같은 데이터베이스 서버(302))에 인증함으로써 참조번호 102에서 시작될 수 있다. 예를 들어, 일부 실시 예들에서, 상기 사용자 장치의 사용자는 임의의 적절한 기법 또는 기법들의 조합을 사용하여 상기 데이터베이스 서버에 연관된 계정에 로그인(log in)할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 사용자는 사용자 인터페이스를 통해 상기 계정에 연관된 사용자 이름 및 패스워드를 입력할 수 있다. 다른 더 구체적인 예로서, 일부 실시 예들에서, 사용자는 사용자에 연관된 생체 정보를 사용하여 상기 계정에 인증될 수 있다. 일부 실시 예들에서, 상기 사용자 장치는 임의의 다른 적합한 인증 기법(들)을 사용하여 상기 데이터베이스 서버에 인증될 수 있다.

[0021] 프로세스(100)는 참조번호 104에서 상기 원격 컴퓨터를 보호하는 방화벽에 IP 주소를 추가하도록 하는 요청에 관련된 정보를 식별할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치가 접속되어야 하는 원격 컴퓨터의 식별자를 결정할 수 있다. 일부 실시 예들에서, 프로세스(100)는 임의의 적절한 기법을 사용하여 상기 원격 컴퓨터의 식별자를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(100)는 사용자 인터페이스를 통해 상기 원격 컴퓨터를 식별하는 이름의 선택사항을 수신함으로써 상기 원격 컴퓨터의 식별자를 결정할 수 있다. 다른 일 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치의 사용자가 원격 접속을 확립하도록 하는 권한을 지닐 수 있는 하나 이상의 원격 컴퓨터들을 식별할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 프로세스(100)는 사용자의 이름에 연관된 특정 원격 컴퓨터를 식별할 수 있다. 다른 더 특정한 예로서, 일부 실시 예들에서, 프로세스(100)는 사용자에 연관된 사용자 유형(예컨대, 사용자가 원격 컴퓨터들 각각에 관한 관리자 권한을 지니는 사용자 유형 및/또는 임의의 다른 적절한 사용자 유형)을 기반으로 다수의 원격 컴퓨터를 식별할 수 있다. 이러한 일부 실시 예들에서, 프로세스(100)는 식별된 원격 컴퓨터(들)의 표시가 사용자에 의한 선택을 위해 (예컨대, 사용자 인터페이스를 통해) 사용자에게 제시되게 할 수 있다.

[0022] 다른 일 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치에 연관된 정보를 결정할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치에 연관된 현재 IP 주소를 결정할 수 있다. 다른 더 구체적인 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치의 지리적 위치(예컨대, 상기 사용자 장치의 현재 위치에 연관된 위도 및/또는 경도, 상기 사용자 장치가 현재 사용자의 사무실에 있지 않음을 표시하는 정보, 및/또는 기타 적절한 지리적 위치)를 결정할 수 있다.

[0023] 또 다른 일 예로서, 일부 실시 예들에서, 프로세스(100)는 현재 IP 주소가 상기 원격 컴퓨터에 연관된 방화벽

규칙들의 리스트에 추가되어야 하거나 현재 IP 주소가 상기 원격 컴퓨터에 연관된 방화벽 규칙들의 리스트에서 제거되어야 하는 것과 같은 상기 요청에 연관된 동작을 결정할 수 있다. 더 특정한 예로서, 사용자 장치가 상기 원격 컴퓨터에 대해 새로운 접속을 확립해야 한다고 프로세스(100)가 결정하는 경우, 현재 IP 주소가 방화벽 규칙들의 리스트에 추가되어야 한다고 프로세스(100)가 결정할 수 있다. 다른 더 특정한 예로서, 상기 원격 컴퓨터에 대한 접속이 (예컨대, 상기 사용자 장치의 사용자로부터의 명시적 입력을 기반으로, 상기 사용자 장치상에서의 작업(activity) 없이 경과하는 소요 시간을 기반으로, 그리고/또는 기타 적절한 정보를 기반으로) 종료되어야 하는 것으로 프로세스(100)가 결정하는 경우에, 프로세스(100)는 현재 IP 주소가 방화벽 규칙들의 리스트에서 제거되어야 하는 것으로 결정할 수 있다.

[0024] 일부 실시 예들에서, 프로세스(100)는 상기 방화벽 규칙들을 수정하도록 하는 요청에 대응하는 임의의 적절한 기준들을 결정할 수 있다. 예를 들어, 상기 요청이 상기 방화벽 규칙들의 리스트에 IP 주소를 추가하는 것일 경우, 프로세스(100)는 상기 요청에 포함되어야 하는 임의의 적절한 타이밍 정보를 결정할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 요청이 유효한 소요 기간(예컨대, 1시간, 2시간, 1일, 1개월, 및/또는 임의의 다른 적절한 소요 기간), IP 주소가 상기 방화벽 규칙들에서 제거되어야 하는 일자 및/또는 시간, IP 주소가 상기 방화벽 규칙들에 포함되어야 하는 시간 윈도우(예컨대, 특정 일자, 특정 요일, 특정 시간 중 오후 1시와 오후 3시 사이의 시간 윈도우, 및/또는 기타 적합한 시간 윈도우), 및/또는 기타 적절한 타이밍 정보를 결정할 수 있다. 다른 더 특정한 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 요청이 유효한 상기 사용자 장치와 상기 원격 컴퓨터 간의 접속 유형들을 결정할 수 있다. 한 특정 예로서, 일부 실시 예들에서, 프로세스(100)는 상기 사용자 장치가 특정 레벨의 암호화 및/또는 암호화 프로토콜을 사용하여, 특정 인증 기법들(예컨대, 멀티-팩터(multi-factor) 인증 및/또는 기타 적절한 기법들)을 사용하여, 그리고/또는 기타 적합한 기준을 사용하여 특정 원격 데스크톱 접속 기법들을 구현하고 있는 경우에 상기 요청이 유효하다고 결정할 수 있다.

[0025] 참조번호 106에서, 프로세스(100)는 식별된 정보를 기반으로 원격 컴퓨터를 보호하는 방화벽을 수정하도록 하는 요청을 생성할 수 있다. 예를 들어, 일부 실시 예들에서, 상기 요청은 상기 원격 컴퓨터의 식별자를 포함할 수 있다. 다른 일 예로서, 일부 실시 예들에서, 상기 요청은 상기 사용자 장치에 연관된 현재 IP 주소를 포함할 수 있다. 또 다른 일 예로서, 일부 실시 예들에서, 상기 요청에는, 현재 IP 주소가 상기 원격 컴퓨터에 대한 접속을 확립하도록 허용된 장치의 IP 주소를 나타내는 방화벽 규칙들의 리스트에 추가되어야 하는지, 방화벽 규칙들의 리스트로부터 제거되어야 하는지, 그리고/또는 기타 적절한 동작을 나타내는 동작 값 매개변수가 포함될 수 있다. 또 다른 일 예로서, 일부 실시 예들에서, 상기 요청에는, 상기 사용자 장치에 연관된 IP 주소가 상기 원격 컴퓨터 장치와의 접속을 확립하도록 허용된 장치의 IP 주소를 나타내는 방화벽 규칙들에 포함되어야 하는 일자 및/또는 시간에 연관된 임의의 적절한 타이밍 정보가 포함될 수 있다. 더 특정한 예로서, 위에서 기재한 바와 같이, 상기 요청에 포함된 타이밍 정보는 IP 주소가 특정한 소용 기간(예컨대, 1시간, 2시간, 1일, 1개월, 및/또는 기타 적절한 소요 시간) 동안, 특정 일자 및/또는 시간까지, 특정 시간 범위(예를 들어, 오후 1시와 오후 5시 사이, 특정 일자의 오후 1시와 다른 일자의 오후 1시 사이, 및/또는 기타 적절한 시간 범위) 동안, 특정 요일(예컨대, 월요일, 요일, 주말, 및/또는 기타 적절한 요일) 동안, 특정 시간(예컨대, 오후 9시 이후, 오전 9시와 오후 5시 사이 그리고/또는 다른 적절한 시간) 동안, 및/또는 기타 적절한 타이밍 정보 또는 타이밍 정보의 조합에 대해 상기 방화벽 규칙에 포함되어야 함을 나타낼 수 있다. 또 다른 특정 예로서, 위에서 기재한 바와 같이, 상기 요청에는 상기 IP 주소가 상기 원격 컴퓨터와의 접속을 확립하도록 허용된 장치의 IP 주소를 나타내는 방화벽 규칙에 포함되어야 하는 경우에 충족되어야 하는 기준이 포함될 수 있다. 더 특정한 예로서, 위에서 기재한 바와 같이, 상기 기준에는 사용되어야 하는 특정 유형의 접속 프로토콜(예컨대, 특정 원격 데스크톱 접속 기법이 사용되어야 하는 프로토콜 및/또는 기타 적절한 프로토콜), 사용되어야 하는 특정 유형의 인증(예컨대, 멀티-팩터 인증, 및/또는 기타 적절한 유형의 인증), 및/또는 기타 적절한 기준이 포함될 수 있다.

[0026] 일부 실시 예들에서, 상기 요청은 방화벽 규칙 이름을 포함될 수 있다. 예를 들어, 일부 실시 예들에서, 상기 방화벽 이름은 상기 요청이 방화벽에 연관된 인바운드 규칙(inbound rule), 방화벽에 연관된 아웃바운드 규칙(outbound rule) 및/또는 기타 적절한 규칙과 관련되어 있음을 나타낼 수 있다. 다른 예로서, 일부 실시 예들에서, 상기 방화벽 이름은 상기 요청이 원격 데스크톱 접속의 확립, 파일 전송, 원격 인쇄, 및/또는 기타 적절한 작업과 같은 상기 원격 컴퓨터상에서의 특정 작업을 수행하는 것과 관련되어 있음을 나타낼 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 상기 방화벽 이름은 상기 요청이 상기 사용자 장치와 상기 원격 컴퓨터 간의 접속에 연관된 특정 포트와 관련되어 있음을 나타낼 수 있다.

[0027] 참조번호 108에서, 프로세스(100)는 상기 데이터베이스 서버에 의한 저장을 위해 상기 요청을 상기 데이터베이

스 서버(예컨대, 도 3에 도시되고 이와 관련지어 이하에 기재되어 있는 바와 같은 데이터베이스 서버(302))에 전송할 수 있다. 일부 실시 예들에서, 프로세스(100)는 임의의 적절한 기법을 사용하여 상기 요청을 상기 데이터베이스 서버에 전송할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(100)는 도 3에 도시되고 이와 관련지어 이하에 기재되어 있는 바와 같은 통신 네트워크를 통해 상기 장치를 상기 데이터베이스 서버에 접속하는 상기 장치에 접속된 네트워크 라우터를 통해 상기 요청을 전송할 수 있다.

[0028] 일부 실시 예들에서, 프로세스(100)는 임의의 적절한 시간에 블록 104로 루프백할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(100)는 블록 104로 루프백하고, 소정 시간이 경과했다는 결정, 상기 장치에 연관된 IP 주소가 변경되었다는 결정, 및/또는 기타 적절한 시점의 결정에 응답하여 원격 컴퓨터에 연관된 방화벽 규칙들을 업데이트하도록 하는 요청을 상기 원격 컴퓨터에 생성하기 위한 정보를 식별할 수 있다. 일부 실시 예들에서, 상기 사용자 장치가 상기 원격 컴퓨터에 접속되어 있는 동안 프로세스(100)가 블록 104로 루프백하는 경우에, 프로세스(100)는 임의의 적절한 정보의 서브세트를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(100)는 블록 104로 루프백할 수 있고 업데이트된 타이밍 정보, 업데이트된 접속 기준, 및/또는 기타 적절한 업데이트된 정보를 결정할 수 있다.

[0029] 도 2를 참조하면, 개시된 주제의 일부 실시 예들에 따른 원격 컴퓨터를 보호하는 방화벽에 대한 방화벽 규칙을 수정하는 프로세스(200)의 일 예가 도시되어 있다. 일부 실시 예들에서, 프로세스(200)의 블록들은 원격 컴퓨터를 보호하는 방화벽 장치(예컨대, 도 3에 도시되고 이와 관련지어 기재되어 있는 바와 같은 방화벽(314))상에서 그리고/또는 방화벽을 사용하는 원격 컴퓨터 장치상에서 실행될 수 있다.

[0030] 프로세스(200)는 상기 원격 컴퓨터에 연관된 방화벽을 수정하도록 하는 요청이 이용 가능한지를 결정하기 위해 데이터베이스 서버(예컨대, 도 3에 도시되고 이와 관련지어 기술되어 있는 바와 같은 데이터베이스 서버(302))에 질의함으로써 참조번호 202에서 시작할 수 있다. 예를 들어, 일부 실시 예들에서, 상기 데이터베이스 서버는 방화벽에 대한 수정 요청을 수신하고 이를 저장하는 데이터베이스 서버일 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 데이터베이스 서버는 도 1과 관련지어 위에 기재한 바와 같이 상기 사용자 장치로부터 상기 사용자 장치의 IP 주소를 포함시키기 위해 방화벽 규칙을 수정하도록 하는 요청을 수신할 수 있다. 일부 실시 예들에서, 프로세스(200)는 상기 데이터베이스 서버에 전송된 질의에 임의의 적절한 정보를 포함할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(200)는 상기 원격 컴퓨터로 안내되는 요청을 식별하기 위해 상기 데이터베이스 서버에 의해 사용될 수 있는 상기 원격 컴퓨터의 식별자를 포함할 수 있다.

[0031] 참조번호 204에서, 프로세스(200)는 상기 원격 컴퓨터로 안내되는 상기 원격 컴퓨터를 보호하는 방화벽을 수정하도록 하는 이용 가능한 요청이 있는지를 결정할 수 있다. 프로세스(200)는 임의의 적절한 정보를 기반으로 이용 가능한 요청이 있는지를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(200)는 상기 데이터베이스 서버로부터 수신된 질의에 대한 응답을 기반으로 이용 가능한 요청이 존재하는지를 결정할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 이용 가능한 요청이 없는 경우에, 프로세스(200)는 상기 데이터베이스 서버로부터 상기 원격 컴퓨터에 상응하는 요청이 발견되지 않았음을 나타내는 응답을 수신할 수 있다. 다른 더 특정한 예로서, 일부 실시 예들에서, 이용 가능한 요청이 있는 경우, 프로세스(200)는 상기 데이터베이스 서버로부터 상기 요청에 상응하는 정보를 포함하는 응답을 수신할 수 있다.

[0032] 프로세스(200)가, 상기 데이터베이스 서버로부터, 특정 사용자 장치로부터 수신된 방화벽 규칙을 수정하도록 하는 요청이 이용 가능함을 나타내는 응답을 수신하는 경우, 상기 응답에는 상기 요청에 상응하는 임의의 적절한 정보가 포함될 수 있다. 예를 들어, 일부 실시 예들에서, 상기 정보에는 상기 사용자 장치에 연관된 현재 IP 주소가 포함될 수 있다. 다른 예로서, 일부 실시 예들에서, 상기 정보에는 특정 방화벽 규칙이 수정되어야 하는 방식을 나타내는 동작 값이 포함될 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 상기 동작 값은 상기 사용자 장치에 연관된 IP 주소가 상기 원격 컴퓨터에 대한 접속을 확립하도록 허용된 장치의 IP 주소를 나타내는 특정 방화벽 규칙에 추가되어야 함을 나타낼 수 있다. 이러한 일부 실시 예들에서, 상기 요청에 포함된 상기 동작 값 및/또는 상기 정보에는 도 1의 블록 104 및 106과 관련지어 위에서 더 구체적으로 기재한 바와 같이 상기 IP 주소가 상기 방화벽 규칙에 포함되어야 하는 기간의 시간을 나타내는 타이밍 정보가 추가로 포함될 수 있다. 다른 더 구체적인 예로서, 일부 실시 예들에서, 상기 동작 값은 상기 사용자 장치에 연관된 IP 주소가 상기 원격 컴퓨터에 대한 접속을 확립하도록 허용된 장치의 IP 주소를 나타내는 특정 방화벽 규칙으로부터 제거되어야 함을 나타낼 수 있다. 또 다른 예로서, 일부 실시 예들에서, 상기 정보에는 하나 이상의 방화벽 규칙 이름들이 포함될 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 방화벽 규칙 이름은 상기 요청이 인바운드 규칙에 그리고/또는 아웃바운드 규칙에 상응함을 나타낼 수 있다. 다른 더 특정한 예로서, 일부 실시 예들에서, 상기 방화벽 규칙 이름은 상기 요청이 원격 데스크톱 접속의 확립, 인쇄, 파일 전송 및/또는 기타 적절한 작업과 같은 특

정 작업에 상응함을 나타낼 수 있다.

[0033] 여기서 유념할 점은 일부 실시 예들에서, 프로세스(200)가 상기 데이터베이스 서버에 질의를 전송하지 않고 상기 데이터베이스 서버로부터 상기 요청에 상응하는 정보를 직접 수신할 수 있다는 점이다. 예를 들어, 일부 실시 예들에서, 상기 데이터베이스 서버는 상기 사용자 장치로부터 수신된 요청을 상기 요청이 안내되는 원격 컴퓨터로 푸시할 수도 있고 상기 사용자 장치로부터 수신된 요청을 상기 사용자 장치로부터 상기 요청을 수신할 때 상기 원격 컴퓨터를 보호하는 방화벽으로 푸시할 수도 있다. 더 특정한 예로서, 일부 실시 예들에서, 상기 데이터베이스 서버는 상기 원격 컴퓨터에 대한 그리고/또는 상기 원격 컴퓨터를 보호하는 방화벽에 대한 접속(예컨대, 가상 사설 네트워크 및/또는 기타 적절한 유형의 접속)을 유지할 수 있고 상기 접속을 사용하여 상기 요청에 상응하는 정보를 전송할 수 있다. 이러한 일부 실시 예들에서, 블록 202 및 204는 생략될 수 있다.

[0034] 참조번호 204에서, 프로세스(200)는 이용 가능한 요청이 없다고 결정하면(참조번호 204에서 "아니오"), 프로세스(200)는 참조번호 212에서 종료될 수 있다.

[0035] 참조번호 204에서, 프로세스(200)는 이용 가능한 요청이 있다고 결정하면(참조번호 204에서 "예"), 프로세스(200)는 상기 요청에 상응하는 방화벽 규칙 이름이 참조번호 206에서 이미 존재하는지를 결정할 수 있다. 여기서 유념할 점은 상기 방화벽 규칙 이름이 인바운드 규칙, 아웃바운드 규칙, 특정 작업에 상응하는 규칙, 및/또는 기타 적합한 규칙과 같은 임의의 적절한 방화벽 규칙 세트에 연관된 이름일 수 있다는 점이다. 프로세스(200)는 방화벽 규칙 이름이 임의의 적절한 방식으로 존재하는지를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(200)는 상기 방화벽 규칙 이름이 방화벽 장치의 메모리 및/또는 상기 원격 컴퓨터의 메모리(예컨대, 도 3 및 도 4에 도시되고 이들과 관련지어 이하에 기재되어 있는 바와 같은, 방화벽(314)의 메모리(404) 및/또는 원격 컴퓨터 (304)의 메모리(404))에 저장된 방화벽 규칙 이름들의 리스트에 포함되어 있는지를 결정할 수 있다. 여기서 유념할 점은 상기 요청에 다수의 방화벽 규칙 이름(예컨대, 인바운드 규칙에 상응하는 제1 방화벽 규칙, 아웃바운드 규칙에 상응하는 제2 방화벽 규칙 이름, 및/또는 기타 적절한 방화벽 규칙 이름)이 포함되는 경우, 다수의 방화벽 규칙 이름 각각이 이미 존재하는지를 프로세스(200)가 결정할 수 있다는 점이다.

[0036] 참조번호 206에서, 프로세스(200)는 상기 방화벽 규칙 이름이 이미 존재한다고 결정하면(참조번호 206에서 "예"), 프로세스(200)는 블록 210으로 진행할 수 있다. 다수의 방화벽 규칙 이름이 상기 요청에 포함되어 있는 경우, 프로세스(200)는 상기 방화벽 규칙 이름들 모두가 이미 존재한다는 결정에 응답하여 블록 210으로 진행할 수 있다.

[0037] 참조번호 206에서, 프로세스(200)는 방화벽 규칙 이름이 아직 존재하지 않는다고 결정하면(참조번호 206에서 "아니오"), 프로세스(200)는 참조번호 208에서 상기 방화벽 규칙 이름에 상응하는 방화벽 규칙을 생성할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(200)는 상기 방화벽 규칙 이름에 상응하는 새로운 리스트를 생성할 수 있다.

[0038] 참조번호 210에서, 프로세스(200)는 상기 요청을 기반으로 상기 방화벽 규칙 이름에 상응하는 방화벽 규칙을 수정할 수 있다. 일부 실시 예들에서, 프로세스(200)는, 상기 방화벽 규칙이 수정되어야 하는 방식을 나타내는 동작 매개변수 값, 타이밍 정보, 기준 정보 및/또는 기타 적절한 정보와 같은, 상기 요청에 포함된 임의의 적절한 정보를 기반으로 상기 방화벽 규칙을 수정할 수 있다. 예를 들어, 프로세스(200)는 상기 사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 한다고 결정하는 경우에, 프로세스(200)는 상기 원격 컴퓨터에 대한 접속을 확립하도록 허용되는 사용자 장치들을 나타내는 IP 주소들의 리스트로부터 상기 IP 주소를 제거할 수 있다. 일부 실시 예들에서, 프로세스(200)는 임의의 적절한 기법 또는 기법들의 조합을 사용하여 상기 사용자 장치의 IP 주소가 상기 방화벽 규칙으로부터 제거되어야 하는지를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 상기 요청에는 (예컨대, 동작 매개변수 값을 기반으로) 상기 방화벽 규칙으로부터 상기 IP 주소를 제거하도록 하는 명시적 명령어가 포함될 수 있다. 다른 예로서, 일부 실시 예들에서, 프로세스(200)는 상기 사용자 장치의 IP 주소가 상기 요청에 포함된 타이밍 정보 또는 기준 정보를 기반으로 상기 방화벽 규칙으로부터 제거되어야 한다고 결정할 수 있다. 더 특정한 예로서, 상기 IP 주소가 상기 방화벽 규칙에 포함되어야 할 시간에 상응하는 타이밍 정보를 상기 요청이 나타내는 경우에, 프로세스(200)는 상기 IP 주소가 상기 방화벽에 포함되어야 할 시간의 외부에 현재 시간이 있는지를 결정할 수 있다. 특정한 예로서, 상기 IP 주소가 특정 일자의 특정 시간까지 상기 방화벽 규칙에 포함되어야 함을 상기 타이밍 정보가 나타내는 경우에, 프로세스(200)는 현재 시간이 상기 특정 시간 및 상기 특정 일자 이후인지를 결정할 수 있다. 다른 더 특정한 예로서, 특정 유형의 접속 프로토콜, 인증 프로토콜 및/또는 암호화 프로토콜이 사용되어야 함을 기준 정보가 나타내는 경우에, 프로세스(200)는 상기 기준이 현재 시간에 충족되지 않는다는 결정에 응답하여 상기 사용자 장치의 IP 주소가 제거되어

야 한다고 결정할 수 있다.

[0039] 다른 예로서, 프로세스(200)는 상기 방화벽 규칙이 상기 사용자 장치의 IP 주소를 포함하도록 수정되어야 한다고 결정하는 경우에, 프로세스(200)는 상기 방화벽 규칙 이름에 상응하는 방화벽 규칙에 상기 IP 주소를 추가할 수 있다. 일부 실시 예들에서, 상기 사용자 장치의 IP 주소를 상기 방화벽 규칙에 추가하기 전에, 프로세스(200)는 임의의 적합한 기준이 만족되는지를 결정할 수 있다. 예를 들어, 일부 실시 예들에서, 프로세스(200)는 상기 IP 주소가 상기 방화벽 규칙에 포함되어야 하는 시간을 특정하는 상기 요청에 포함된 타이밍 정보에 표시된 시간 범위 내에 현재 시간이 있는지 여부를 결정할 수 있고, 현재 시간이 상기 시간 범위에 포함된다는 결정에 응답하여 상기 IP 주소를 포함시키도록 상기 방화벽 규칙을 수정할 수 있다. 다른 예로서, 일부 실시 예들에서, 프로세스(200)는 상기 사용자 장치와의 접속에 연관된 기준이 충족되는지를 결정할 수 있다. 더 특정한 예로서, 일부 실시 예들에서, 프로세스(200)는 상기 사용자 장치가 특정 유형 또는 레벨의 암호화, 특정 유형 또는 레벨의 인증, 특정 유형의 원격 데스크톱 프로토콜, 및/또는 기타 적합한 기준을 사용하고 있는지를 결정할 수 있고, 상기 기준이 충족된다는 결정에 응답하여 상기 방화벽 규칙에 상기 사용자 장치의 IP 주소를 추가할 수 있다. 다른 더 특정한 예로서, 일부 실시 예들에서, 프로세스(200)는 상기 사용자 장치의 위치가 특정 지리적 정보를 충족시키는지(예컨대, 상기 사용자 장치가 현재 특정 지리적 영역 내에 있는지, 상기 사용자 장치가 현재 특정 지리적 영역 내에 있지 않은지, 그리고/또는 기타 적절한 지리적 정보)를 결정할 수 있다. 특정한 예로서, 일부 실시 예들에서, 프로세스(200)는 상기 사용자 장치가 현재 특정 위치나 특정 그룹의 위치들(예컨대, 특정 그룹의 나라들, 그리고/또는 기타 적절한 그룹의 위치들)에 있음을 상기 사용자 장치의 위치를 나타내는 지리적 정보가 나타낸다는 결정에 응답하여 상기 사용자 장치의 IP 주소가 상기 방화벽 규칙에 추가되어야 함을 결정할 수 있다.

[0040] 여기서 유념할 점은 일부 실시 예들에서, 방화벽 규칙을 수정하기 전에 임의의 적절한 기준이 충족되는지를 결정하는 것이 데이터베이스 서버에 의해 수행될 수 있다는 점이다. 예를 들어, 일부 실시 예들에서, 상기 데이터베이스 서버는 타이밍 정보, 접속 정보, 지리 정보, 및/또는 기타 적절한 정보에 관련된 기준이 충족되는지를 결정할 수 있고, 상기 기준이 충족되지 않으면 상기 데이터베이스 서버는 상기 방화벽 장치 및/또는 상기 원격 컴퓨터로 요청을 전송하지 않고 상기 요청을 삭제할 수 있다.

[0041] 프로세스(200)는 참조번호 212에서 종료될 수 있다. 추가로나 대안으로, 일부 실시 예들에서, 프로세스(200)는 블록 202로 루프백할 수 있고 방화벽 규칙을 수정하도록 하는 추가적이거나 또는 업데이트된 요청이 수신되었는지를 결정하기 위해 상기 데이터베이스 서버에 질의할 수 있다.

[0042] 도 3을 참조하면, 개시된 주제의 일부 실시 예들에 따른 사용될 수 있는 방화벽 규칙을 수정하기 위한 하드웨어(300)의 일 예가 도시되어 있다. 도시된 바와 같이, 하드웨어(300)는 데이터베이스 서버(302), 원격 컴퓨터(304), 통신 네트워크(306), 사용자 장치들(310, 312)과 같은 하나 이상의 사용자 장치들(308), 및/또는 방화벽(314)을 포함할 수 있다.

[0043] 데이터베이스 서버(302)는 원격 컴퓨터(304)를 보호하는 방화벽을 수정하기 위한 정보를 저장하는 임의의 적절한 서버(들)일 수 있다. 예를 들어, 일부 실시 예들에서, 데이터베이스 서버(302)는 도 1과 관련지어 위에서 기재한 바와 같이 원격 컴퓨터(304)에 대한 원격 접속을 확립하려고 시도하는 사용자 장치(308)로부터 요청을 수신할 수 있다. 다른 예로서, 일부 실시 예들에서, 데이터베이스 서버(302)는 도 3와 관련지어 위에서 기재한 바와 같이 저장된 요청들 및/또는 저장된 요청들에 상응하는 정보를 원격 컴퓨터(304)에 전송할 수 있다.

[0044] 원격 컴퓨터(304)는 사용자 장치(308)로부터 액세스 요청을 수신하는 임의의 적절한 장치일 수 있다. 예를 들어, 일부 실시 예들에서, 사용자 장치(308)는 원격 컴퓨터(304)와의 원격 데스크톱 접속을 확립할 수 있다. 일부 실시 예들에서, 원격 컴퓨터(304)는 도 2와 관련지어 위에서 기재한 바와 같이 방화벽(314)에 의해 보호될 수 있다.

[0045] 통신 네트워크(306)는 일부 실시 예들에서 하나 이상의 유선 및/또는 무선 네트워크들의 임의의 적절한 조합일 수 있다. 예를 들어, 통신 네트워크(306)는 인터넷, 인트라넷, WAN(wide-area network), LAN(local-area network), 무선 네트워크, DSL(digital subscriber line) 네트워크, 프레임 릴레이 네트워크, ATM(asynchronous transfer mode) 네트워크, VPN(virtual private network), 및/또는 기타 적절한 통신 네트워크 중의 어느 하나 또는 그 이상을 포함할 수 있다. 사용자 장치(308)는 하나 이상의 통신 링크에 의해, 하나 이상의 통신 링크를 통해 데이터베이스 서버(302) 및 원격 컴퓨터(304)에 링크될 수 있는 통신 네트워크(306)에 접속될 수 있다. 상기 통신 링크는 네트워크 링크, 다이얼-업 링크, 무선 링크, 고정-배선 링크, 기타 적절한 통신 링크, 또는 그러한 링크들의 임의의 적절한 조합과 같은, 사용자 장치(308), 데이터베이스 서버(302) 및

원격 컴퓨터(304) 간에 데이터를 통신하기에 적합한 임의의 통신 링크일 수 있다. 일부 실시 예들에서, 통신 네트워크(306)를 통한 통신은 전송 제어 프로토콜(Transmission Control Protocol; TCP), 사용자 데이터그램 프로토콜(User Datagram Protocol; UDP), 및/또는 기타 적절한 프로토콜과 같은 임의의 적절한 유형의 통신 프로토콜에 상응하는 전송된 네트워크 패킷들을 통해 이루어질 수 있다.

[0046] 사용자 장치(308)는 데이터베이스 서버(302) 및/또는 원격 컴퓨터(304)와 통신하기에 적합한 임의의 하나 이상의 사용자 장치들(예컨대, 사용자 장치(310 및/또는 312))을 포함할 수 있다. 예를 들어, 일부 실시 예들에서, 사용자 장치(308)는 모바일폰, 태블릿 컴퓨터, 웨어러블 컴퓨터, 랩톱 컴퓨터, 차량(예컨대, 자동차, 보트, 비행기 또는 기타 적절한 차량) 정보 및/또는 엔터테인먼트 시스템, 및또는 기타 적절한 모바일 장치와 같은 모바일 장치를 포함할 수 있다. 다른 예로서, 일부 실시 예들에서, 사용자 장치(308)는 텔레비전, 프로젝터 장치, 게임 콘솔, 데스크톱 컴퓨터, 및/또는 기타 적합한 비-모바일 장치와 같은 비-모바일 장치를 포함할 수 있다. 일부 실시 예들에서, 사용자 장치(308)는 원격 컴퓨터(304)와의 원격 데스크톱 접속을 확립할 수 있다.

[0047] 일부 실시 예들에서, 방화벽(314)은 원격 컴퓨터(304)를 보호하기 위한 임의의 적절한 장치일 수 있다. 예를 들어, 일부 실시 예들에서, 방화벽(314)은 원격 컴퓨터와의 접속을 확립하도록 허용되는 사용자 장치 및/또는 원격 컴퓨터(304)와의 접속을 확립하지 못하도록 차단되는 사용자 장치에 연관된 IP 주소들의 리스트를 저장 및 유지하는 장치일 수 있다. 여기서 유념할 점은 비록 방화벽(314)이 원격 컴퓨터(304)와 분리된 장치로서 도시되어 있지만, 일부 실시 예들에서, 방화벽(314)이 원격 컴퓨터(304)와 결합될 수 있다는 점이다.

[0048] 비록 데이터베이스 서버(302) 및 원격 컴퓨터(304)가 2개의 장치로서 도시되어 있지만, 데이터베이스 서버(302) 및/또는 원격 컴퓨터(304)에 의해 수행되는 기능들은 일부 실시 예들에서 임의의 적절한 개수의 장치들(단지 하나만을 포함함)을 사용하여 수행될 수 있다. 예를 들어, 일부 실시 예들에서는, 데이터베이스 서버(302) 및/또는 원격 컴퓨터(304)에 의해 수행되는 기능들을 구현하기 위해 한 개, 세개 또는 그 이상의 장치들이 사용될 수 있다.

[0049] 비록 도면을 지나치게 복잡하게 하는 것을 회피하기 위해 2개의 사용자 장치(310, 312)가 도 3에 도시되어 있지만, 임의의 적절한 개수의 사용자 장치들(단지 하나만을 포함함), 및/또는 임의의 적절한 유형의 사용자 장치들이 일부 실시 예들에서 사용될 수 있다.

[0050] 데이터베이스 서버(302), 원격 컴퓨터(304), 및 사용자 장치(308)는 일부 실시 예들에서 임의의 적절한 하드웨어를 사용하여 구현될 수 있다. 예를 들어, 일부 실시 예들에서, 장치들(302, 304 및/또는 308)은 임의의 적절한 범용 컴퓨터 또는 전용 컴퓨터를 사용하여 구현될 수 있다. 예를 들어, 모바일폰은 전용 컴퓨터를 사용하여 구현될 수 있다. 이러한 임의의 범용 컴퓨터 또는 전용 컴퓨터는 임의의 적절한 하드웨어를 포함할 수 있다. 예를 들어, 도 4의 대표적인 하드웨어(400)에 도시된 바와 같이, 이러한 하드웨어는 하드웨어 프로세서(402), 메모리 및/또는 저장 장치(404), 입력 장치 제어기(406), 입력 장치(408), 디스플레이/오디오 드라이버(410), 디스플레이 및 오디오 출력 회로(412), 통신 인터페이스(들)(414), 및 안테나(416), 및 버스(418)를 포함할 수 있다.

[0051] 하드웨어 프로세서(402)는 일부 실시 예들에서 마이크로프로세서, 마이크로컨트롤러, 디지털 신호 프로세서(들), 전용 로직 및/또는 범용 컴퓨터 또는 전용 컴퓨터의 기능을 제어하기 위한 기타 적절한 회로와 같은 임의의 적합한 하드웨어 프로세서를 포함할 수 있다. 일부 실시 예들에서, 하드웨어 프로세서(402)는 사용자 장치(308)의 메모리 및/또는 저장 장치(404)에 저장된 컴퓨터 프로그램에 의해 제어될 수 있다. 예를 들어, 일부 실시 예들에서, 상기 컴퓨터 프로그램은 하드웨어 프로세서(402)가 도 1과 관련지어 위에서 기재한 바와 같은 프로세스(또는 그의 일부)를 수행하게 할 수 있다. 일부 실시 예들에서, 하드웨어 프로세서(402)는 원격 컴퓨터(304) 및/또는 방화벽(314)의 메모리 및/또는 저장 장치(404)에 저장된 컴퓨터 프로그램에 의해 제어될 수 있다. 예를 들어, 일부 실시 예들에서, 상기 컴퓨터 프로그램은 하드웨어 프로세서(402)가 도 2와 관련지어 기재한 한 바와 같은 프로세스(또는 그의 일부)를 수행하게 한다.

[0052] 메모리 및/또는 저장 장치(404)는 일부 실시 예들에서 프로그램, 데이터, 미디어 컨텐츠, 및/또는 기타 적절한 정보를 저장하기 위한 임의의 적절한 메모리 및/또는 저장 장치일 수 있다. 예를 들어, 메모리 및/또는 저장 장치(404)는 랜덤 액세스 메모리, 판독 전용 메모리, 플래시 메모리, 하드 디스크 저장 장치, 광학 매체, 및/또는 기타 적절한 메모리를 포함할 수 있다.

[0053] 입력 장치 제어기(406)는 일부 실시 예들에서 하나 이상의 입력 장치들(408)로부터의 입력을 제어 및 수신하기 위한 임의의 적절한 회로일 수 있다. 예를 들어, 입력 장치 제어기(406)는 터치 스크린, 키보드, 마우스, 하나

이상의 버튼들, 음성 인식 회로, 마이크로폰, 카메라, 광학 센서, 가속도계, 온도 센서, 근접장 센서, 및/또는 기타 유형의 입력 장치로부터의 입력을 수신하기 위한 회로일 수 있ㄷ다.

[0054] 디스플레이/오디오 드라이버(410)는 일부 실시 예들에서 하나 이상의 디스플레이/오디오 출력 장치들(412)로의 출력을 제어 및 구동하기 위한 임의의 적절한 회로일 수 있다. 예를 들어, 디스플레이/오디오 드라이버(410)는 터치 스크린, 평판 디스플레이, 음극선관 디스플레이, 프로젝터, 스피커 또는 스피커들, 및/또는 기타 적절한 디스플레이 및/또는 프리젠테이션 장치를 구동하기 위한 회로일 수 있다.

[0055] 통신 인터페이스(들)(414)는 도 3에 도시된 바와 같은 네트워크(306)와 같은 하나 이상의 통신 네트워크들과 인터페이스하기 위한 임의의 적절한 회로일 수 있다. 예를 들어, 인터페이스(들)(414)는 네트워크 인터페이스 카드 회로, 무선 통신 회로, 및/또는 기타 적합한 유형의 통신 네트워크 회로를 포함할 수 있다.

[0056] 안테나(416)는 일부 실시 예들에서 통신 네트워크(예컨대, 통신 네트워크(306))와 무선으로 통신하기 위한 임의의 적절한 하나 이상의 안테나들일 수 있다. 일부 실시 예들에서, 안테나(416)는 생략될 수 있다.

[0057] 버스(418)는 일부 실시 예들에서 2개 이상의 구성요소들(402, 404, 406, 410, 414) 간의 통신을 위한 임의의 적절한 메커니즘일 수 있다.

[0058] 일부 실시 예들에 의하면, 기타 적절한 구성요소들이 하드웨어(400)에 포함될 수 있다.

[0059] 일부 실시 예들에서, 위에서 기재한 도 1 및 도 2의 프로세스들의 블록들 중 적어도 일부는 도 1 및 도 2에 도시되고 이들과 관련지어 기재되어 있는 순서 및 시퀀스에 국한되지 않는 임의의 순서 및 시퀀스로 실행 또는 수행될 수 있다. 또한, 위에서 기재한 도 1 및 도 2의 블록들 중 일부는, 대기시간 및 처리시간을 줄이기 위해 적절한 경우에 실질적으로 동시에 또는 병렬로 실행되거나 수행될 수 있다. 추가로나 대안으로, 위에서 기재한 도 1 및 도2의 프로세스들의 블록들 중 일부가 생략될 수 있다.

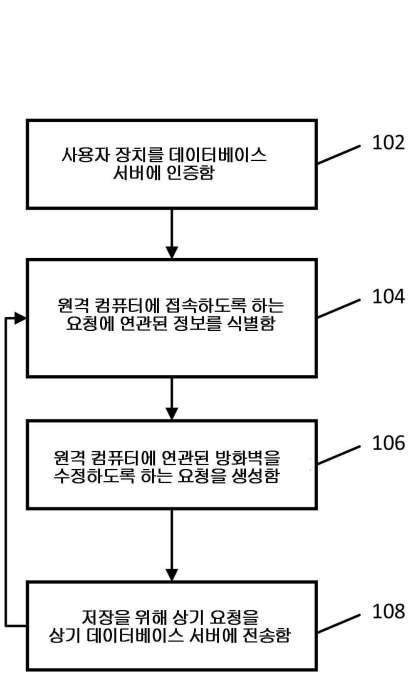
[0060] 일부 실시 예들에서, 본원 명세서에 기재된 기능들 및/또는 프로세스들을 수행하기 위한 명령어들을 저장하기 위해 임의의 적절한 컴퓨터 판독가능 매체가 사용될 수 있다. 예를 들어, 일부 실시 예들에서, 컴퓨터 판독가능 매체는 일시적이거나 비-일시적일 수 있다. 예를 들어, 비-일시적 컴퓨터 판독가능 매체는 비-일시적 형태의 자기 매체(예컨대, 하드 디스크, 플로피 디스크, 및/또는 기타 적절한 자기 매체), 비-일시적 형태의 광학 매체(예컨대, 콤팩트 디스크, 디지털 비디오 디스크, 블루-레이 디스크, 및/또는 기타 적절한 광학 매체), 비-일시적 형태의 반도체 매체(예컨대, 플래시 메모리, 전기적으로 프로그램가능한 판독 전용 메모리(electrically programmable read-only memory; EPROM), 전기적으로 소거가능하고 프로그램가능한 판독 전용 메모리(electrically erasable programmable read-only memory; EEPROM), 및/또는 기타 적절한 반도체 매체), 전송 중에 임의의 영속성 외형이 일시적이지 않거나 결여되어 있지 않은 임의의 적절한 매체, 및/또는 적절한 유형(有形)의 매체와 같은 매체를 포함할 수 있다. 다른 예로서, 일시적 컴퓨터 판독가능 매체는 네트워크상의 신호, 와이어, 도체, 광섬유, 회로의 신호, 전송 중에 영속성 외형이 일시적이거나 결여된 임의의 적절한 매체, 및/또는 임의의 적절한 무형의 매체를 포함할 수 있다.

[0061] 따라서, 동적 IP 주소를 기반으로 방화벽 규칙을 수정하는 방법, 시스템 및 매체가 제공된다.

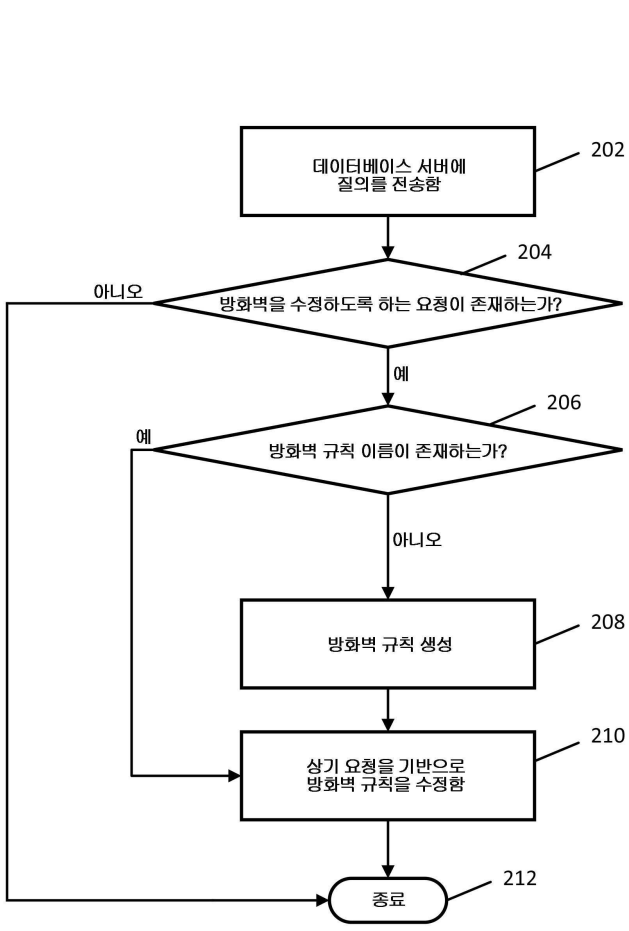
[0062] 비록 본 발명이 전술한 전형적인 실시 예들에서 기재되고 도시되었지만, 여기서 이해할 점은 본 개시내용이 단지 예로만 이루어졌으며, 본 발명의 구현의 세부사항의 많은 변경이 이하의 청구범위에 의해서만 제한되는, 본 발명의 사상 및 범위를 벗어나지 않고 이루어질 수 있다는 점이다. 개시된 실시 예들의 특징들은 다양한 방식으로 조합 및 재배열될 수 있다.

도면

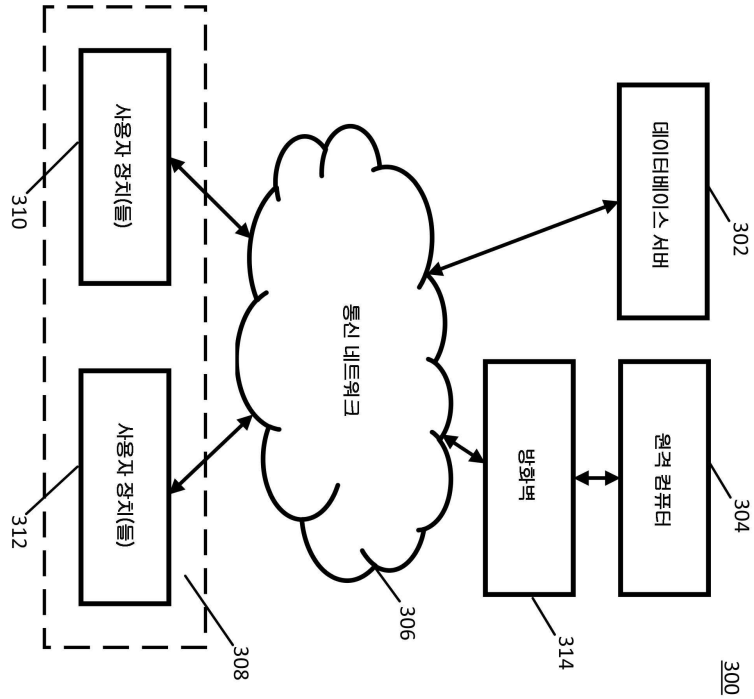
도면1


100
사용자 장치를 데이터베이스 서버에 인증함
102
원격 컴퓨터에 접속하도록 하는 요청에 연관된 정보를 식별함
104
원격 컴퓨터에 연관된 방화벽을 수정하도록 하는 요청을 생성함
106
저장을 위해 상기 요청을 상기 데이터베이스 서버에 전송함
108

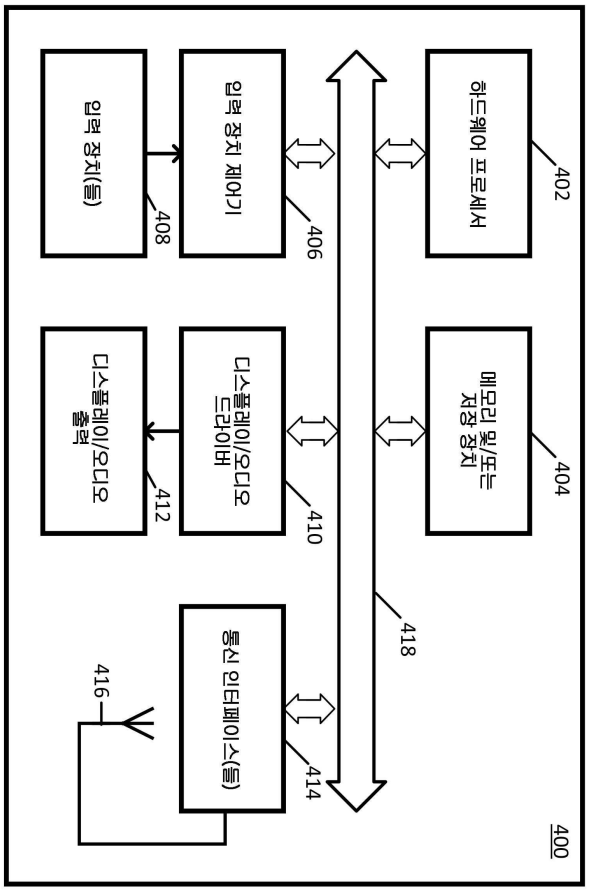
도면2


200
데이터베이스 서버에 질의를 전송함
202
방화벽을 수정하도록 하는 요청이 존재하는가?
204
아니오
예
방화벽 규칙 이름이 존재하는가?
206
예
아니오
방화벽 규칙 생성
208
상기 요청을 기반으로 방화벽 규칙을 수정함
210
종료
212

도면3


사용자 장치(들)
310
사용자 장치(들)
312
308
통신 네트워크
306
데이터베이스 서버
302
방화벽
314
원격 컴퓨터
304
300

도면4


입력 장치(들)
408
입력 장치 제어기
406
하드웨어 프로세서
402
디스플레이/오디오 출력
412
디스플레이/오디오 드라이버
410
메모리 및/또는 저장 장치
404
418
416
통신 인터페이스(들)
414
400