(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년06월27일
(11) 등록번호 10-1872072
(24) 등록일자 2018년06월21일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
H04L 63/1425 (2013.01)
H04L 67/06 (2013.01)
(21) 출원번호 10-2015-0100485
(22) 출원일자 2015년07월15일
심사청구일자 2016년06월08일
(65) 공개번호 10-2017-0009073
(43) 공개일자 2017년01월25일
(56) 선행기술조사문헌
US20110219452 A1*
KR100417654 B1*
KR101348285 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 엘지유플러스
서울특별시 용산구 한강대로 32(한강로3가)
(72) 발명자
오충목
서울특별시 용산구 한강대로 32 (한강로3가)
(74) 대리인
특허법인 무한

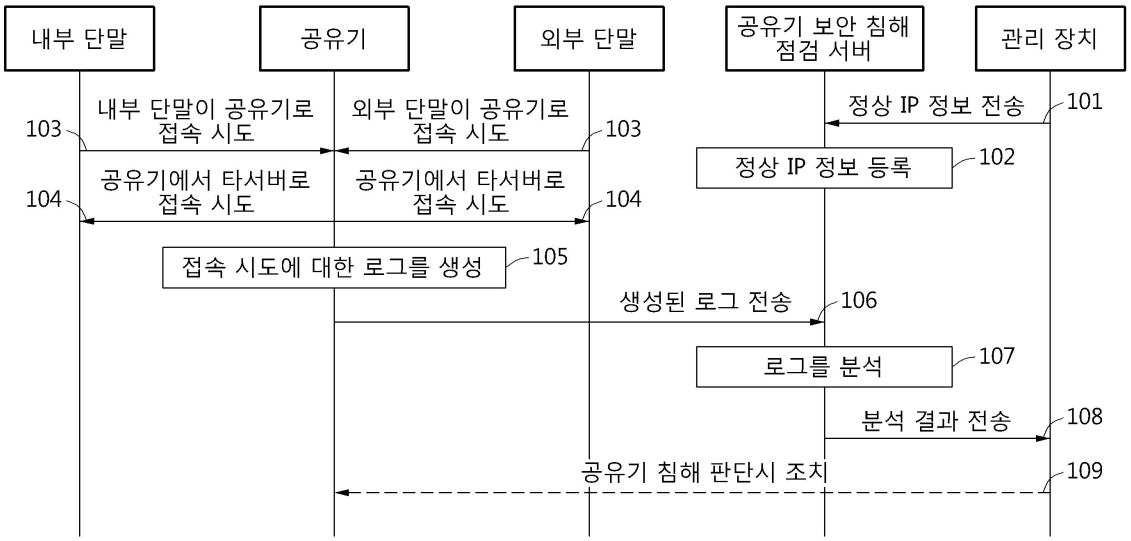
전체 청구항 수 : 총 5 항 심사관 : 문형섭

(54) 발명의 명칭 **공유기 보안 침해 점검 방법 및 이를 수행하는 시스템**

(57) 요 약

이하의 실시예는 공유기의 보안 침해를 점검하는 방법과 이를 수행하는 시스템에 관한 것이다. 보안 침해 점검 서버에서 수행되는 공유기 보안 침해 점검 방법에 있어서, 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 단계; 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계; 상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 단계; 및 상기 로그의 분석 결과를 상기 보안 침해 관리 장치로 전송하는 단계를 포함하는, 공유기 보안 침해 점검 방법이 제공될 수 있다.

대 표 도



(52) CPC특허분류
H04L 2463/144 (2013.01)

명 세 서

청구범위

청구항 1

보안 침해 점검 서버에서 수행되는 공유기 보안 침해 점검 방법에 있어서,

보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 단계;

공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계;

상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 단계; 및

상기 로그의 분석 결과를 상기 보안 침해 관리 장치로 전송하는 단계

를 포함하고

상기 로그는

상기 공유기의 IP(DST)로 접속을 하는 패킷의 수신에 관한 제1 로그 및 상기 공유기의 IP(SRC)를 이용하여 타 서버로 접속을 하는 패킷의 전송에 관한 제2 로그를 포함하며,

상기 수신된 로그를 분석하는 단계는

상기 제1 로그의 경우,

상기 정상 IP 정보를 이용하여 상기 제1 로그의 정상 IP 및 비정상 IP를 분류함으로써, 상기 공유기가 침해되었는지 여부를 판단하는 단계; 및

상기 제2 로그의 경우,

상기 타 서버가 외부 IP를 가지는 외부 서버인지 여부를 판단하는 단계;

상기 타 서버가 외부 서버인 경우, 상기 정상 IP 정보를 이용하여 상기 외부 IP가 정상 IP인지 여부를 판단하는 단계; 및

상기 외부 IP가 비정상 IP인 경우, 상기 외부 IP가 이상 IP에 해당하는지 여부, 상기 외부 IP로의 접속 빈도, 및 상기 외부 IP와 동일한 IP로의 접속 이력 중 적어도 하나를 분석함으로써, 상기 공유기가 침해되었는지 여부를 판단하는 단계

를 포함하는,

공유기 보안 침해 점검 방법.

청구항 2

제1항에 있어서,

상기 보안 침해 관리 장치로부터 수신하는 상기 정상 IP 정보는,

프로비저닝 서버, 업그레이드 서버 및 단말 관리 서버를 포함하는 상기 정상 IP 정보인 것을 특징으로 하는,

공유기 보안 침해 점검 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계는,

미리 정해진 주기로 FTP (File transfer protocol)을 포함하는 방식으로 상기 공유기로부터 대용량의 상기 로그를 수신하는 것을 특징으로 하는,

공유기 보안 침해 점검 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

공유기 보안 침해 점검 방법을 위한 보안 침해 점검 서버에 있어서,

보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 등록부;

공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 수신부;

상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 분석부; 및

상기 로그의 분석 결과를 상기 보안 침해 관리 장치로 전송하는 전송부

를포함하고

상기 로그는

상기 공유기의 IP(DST)로 접속을 하는 패킷의 수신에 관한 제1 로그 및 상기 공유기의 IP(SRC)를 이용하여 타 서버로 접속을 하는 패킷의 전송에 관한 제2 로그를 포함하며,

상기 수신된 로그를 분석하는 단계는

상기 제1 로그의 경우,

상기 정상 IP 정보를 이용하여 상기 제1 로그의 정상 IP 및 비정상 IP를 분류함으로써, 상기 공유기가 침해되었는지 여부를 판단하는 단계; 및

상기 제2 로그의 경우,

상기 타 서버가 외부 IP를 가지는 외부 서버인지 여부를 판단하는 단계;

상기 타 서버가 외부 서버인 경우, 상기 정상 IP 정보를 이용하여 상기 외부 IP가 정상 IP인지 여부를 판단하는 단계; 및

상기 외부 IP가 비정상 IP인 경우, 상기 외부 IP가 이상 IP에 해당하는지 여부, 상기 외부 IP로의 접속 빈도, 및 상기 외부 IP와 동일한 IP로의 접속 이력 중 적어도 하나를 분석함으로써, 상기 공유기가 침해되었는지 여부를 판단하는 단계

를 포함하는

공유기 보안 침해 점검 서버.

청구항 8

제7항에 있어서,

상기 등록부는,

프로비저닝 서버, 업그레이드 서버 및 단말 관리 서버를 포함하는 상기 정상 IP 정보를 수신하는,

공유기 보안 침해 점검 서버.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 이하의 실시예는 공유기의 보안 침해를 점검하는 방법과 이를 수행하는 시스템에 관한 것이다.

배 경 기 술

[0003] 최근, 무선 네트워크에 대한 수요는 노트북, 태블릿, 스마트폰 등을 포함하여 점점 증가하는 추세에 있다. 이에 더불어, 원격 근무자나 사내에서 근무하는 직원이 이동하면서 편리하게 기업 내 네트워크를 사용할 수 있도록 기업 내 무선랜의 도입이 꾸준히 증가하고 있다.

[0004] 그러나, 보통의 공유기는 보안에 취약하여, 공유기에 연결된 단말이 외부의 공격에 의해 침해될 수 있고, 또는 공유기 자체가 디도스 봇(DDos Bot)이 될 수 있으므로, 보안을 점검하기 위한 기능이 필요하다.

[0005] 기존에 제공되는 공유기의 보안 점검을 위한 발명으로, 리눅스(Linux) 서버 보안 툴을 적용하는 방법이 제공되고 있으나 저가, 저스펙의 공유기에서는 수행하기 어려운 툴이며, 공유기의 기능을 제공하기 위해 오픈 소스 아이피테이블(Open Source IPtables)이 제공되고 있으나, 접근 제어용으로만 사용되고 있으며, 로그(Log)를 이용한 상세 분석 기능은 제공되지 않는다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예를 통해서 일반적으로 보안에 취약한 공유기에 대해서 공유기 접속 로그를 분석함으로써 공유기 보안의 침해 여부를 판단하기 위한 공유기 보안 침해 점검 방법 및 그 시스템을 제공한다.

[0008] 또한, 공유기 공격에 대해 사전에 감지하고, 이미 침해된 공유기 정보를 제공함으로써 공유기의 보안을 강화하고, 보다 안전한 인터넷 사용이 가능하도록 한다.

과제의 해결 수단

[0010] 보안 침해 점검 서버에서 수행되는 공유기 보안 침해 점검 방법에 있어서, 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 단계; 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계; 상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 단계; 및 상기 로그의 분석 결과를 상기 보안 침해 관리 장치로 전송하는 단계를 포함하는, 공유기 보안 침해 점검 방법이 제공될 수 있다.

[0011] 일측에 있어서, 상기 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 단계는, 프로비저닝 서버, 업그레이드 서버 및 단말 관리 서버를 포함하는 상기 정상 IP 정보를 수신하는 단계를 포함할 수 있다.

[0012] 또 다른 측면에 있어서, 상기 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계는, 외부에서 상기 공유기의 IP로 접속 시도에 대한 패킷 및 상기 공유기의 IP를 통해 타 서버로의 접속 시도에 대한 패킷 중 적어도 하나에 대해 생성된 로그를 수신하는 단계를 포함할 수 있다.

[0013] 또 다른 측면에 있어서, 상기 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 단계는, 미리 정해진 주기로 FTP (File transfer protocol)을 포함하는 방식으로 상기 공유기로부터 대용량의 상기 로그를 수신하는 단계를 포함할 수 있다.

[0014] 또 다른 측면에 있어서, 상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 단계는, 상기 수신된 정상 IP 정보를 기준으로, 상기 수집된 로그의 정상 IP 및 비정상 IP를 분류하는 단계를 포함할 수 있다.

[0015] 또 다른 측면에 있어서, 상기 비정상 IP에 대해서, 외부 IP 접속, 접속 빈도 및 동일 IP 접속 이력 중 적어도 하나를 분석하는 단계를 더 포함할 수 있다.

[0016] 공유기 보안 침해 점검 방법을 위한 보안 침해 점검 서버에 있어서, 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록하는 등록부; 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신하는 수신부; 상기 정상 IP 정보를 이용하여 상기 수신된 로그를 분석하는 분석부; 및 상기 로그의 분석 결과를 상기 보안 침해 관리 장치로 전송하는 전송부를 포함하는, 공유기 보안 침해 점검 서버가 제공될 수 있다.

발명의 효과

[0018] 본 발명의 실시예를 통해서 일반적으로 보안에 취약한 공유기에 대해서 공유기 접속 로그를 분석함으로써 공유기 보안의 침해 여부를 판단하기 위한 공유기 보안 침해 점검 방법 및 그 시스템을 제공할 수 있다.

[0019] 또한, 공유기 공격에 대해 사전에 감지하고, 이미 침해된 공유기 정보를 제공함으로써 공유기의 보안을 강화하고, 보다 안전한 인터넷 사용이 가능하다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 방법을 수행하는 공유기 보안 침해 점검 시스템의 동작을 설명하기 위한 흐름도이다.

도 2는 본 발명의 일실시예에 있어서, 공유기에서 로그가 생성되는 경우에 대해 설명하기 위한 도면이다.

도 3은 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 서버를 통해 수행되는 공유기 보안 침해 점검 방법을 설명하기 위한 흐름도이다.

도 4는 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 방법을 수행하는 공유기 보안 침해 점검 서버의 구성을 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 공유기 보안 침해 점검 방법 및 이를 수행하는 시스템에 대해서 첨부된 도면을 참조하여 자세히 설명하도록 한다.

[0023] 아래 설명하는 실시예들에는 다양한 변경이 가해질 수 있다. 아래 설명하는 실시예들은 실시 형태에 대해 한정하려는 것이 아니며, 이들에 대한 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0024] 실시예에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 실시예를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0025] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0026] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0028] 도 1은 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 방법을 수행하는 공유기 보안 침해 점검 시스템의 동작을 설명하기 위한 흐름도이다.

[0029] 실시예에 따른 공유기는, 웹 서비스 서버와 같이 서비스를 제공하는 서버가 아닌 홈 게이트웨이(Gateway)로 활용하는 장비로써, 일반 사용자는 공유기 설정(Config)을 변경하는 경우 이외에는 접속하지 않을 수 있다. 예컨대, 주로 와이파이(Wifi) SSID(subsystem identification) 비밀번호를 변경할 때에 접속하며, 일반 사용자는 공유기를 디폴트(Default)로 사용할 수 있다.

[0030] 내부 단말은 공유기로 접속하는 스마트폰, 태블릿, 노트북 등의 무선 통신 기기를 포함하여, 사내 등에서 공유기로 직접 연결하는 단말에 해당할 수 있고, 외부 단말은 다른 네트워크를 통해 공유기로 접속하는 무선 통신 기기에 해당하며, 원격 단말을 포함할 수 있다.

[0031] 단계(101)에서, 관리 장치는 정상 IP 정보를 공유기 보안 침해 점검 서버로 전송할 수 있다.

[0032] 실시예에서, 관리 장치는 공유기의 프로비저닝(Provisioning) 서버, 업그레이드 서버, 단말 관리 서버 등의 IP에 대해서 정상 IP 정보로 제공하여, 이후 공유기 침해 점검 시 정상 및 비정상 분류 기준으로 이용될 수 있도록 한다.

[0033] 단계(102)에서, 공유기 보안 침해 점검 서버는 수신된 정상 IP 정보를 등록할 수 있다.

[0034] 공유기 보안 침해 점검 서버에 정상 IP 정보가 등록된 이후, 공유기는 발생하는 접속 시도에 대해서 로그를 발생시킬 수 있다.

[0035] 단계(103) 및 단계(104)에서, 공유기에서 접속 시도가 발생할 수 있다.

[0036] 단계(103)와 같이, 외부 또는 내부 단말이 공유기로 접속을 시도할 수 있고, 단계(104)와 같이 공유기에서 타 서버로 접속을 시도할 수 있다. 실시예에서, 단계(103) 및 단계(104) 중 적어도 하나의 접속 시도가 발생할 수 있다.

[0037] 예를 들어, 내부 단말에서 공유기를 통해 웹 사이트에 접속할 수 있으며, 내부 및 외부 단말에서 공유기로 접속할 수 있고, 공유기에서 내부 다른 서버로 접속하거나 외부 서버로 접속할 수 있다.

[0038] 단계(105)에서 공유기는 접속 시도에 대해서 로그를 생성할 수 있다.

[0039] 실시예에서, 공유기에서 NAT(Network Address Translation)나 포워딩(Forwarding) 패킷에 대해서는 로그를 생성하지 않으며, 공유기의 IP(DST)로 접속을 시도하는 패킷 및 공유기의 IP(SRC)를 이용하여 타 서버로 접속을 시도하는 패킷에 대해서 로그를 생성할 수 있다.

[0040] 공유기에서 로그가 생성되는 경우에 대해서 도 2를 통해 자세히 설명하도록 한다.

[0042] 도 2는 본 발명의 일실시예에 있어서, 공유기에서 로그가 생성되는 경우에 대해 설명하기 위한 도면이다.

[0043] 도 2(a)는 정상적인 공유기를 사용하는 경우에 관한 것이고, 도 2(b)는 외부 및 내부에서 공유기로 접근 시도하는 경우에 관한 것이며, 도 2(c)는 공유기에서 타 서버로 접근을 시도하는 경우에 관한 것이다.

[0044] 앞서 간단히 설명했듯이, 도 2(a)와 같이, 공유기를 정상적으로 사용하는 NAT(Network Address Translation)나 포워딩(Forwarding) 패킷에 대해서는 네트워크 사용 로그를 생성하지 않는다. 예컨대, PC, 노트북이나 스마트폰 등 사용자 단말로 공유기를 통해 네트워크를 이용하여 "naver", "youtube", "daum" 등의 웹사이트에 접속하는 동작에 해당할 수 있다.

[0045] 도 2(b)의 실시예에 따르면, 사용자 단말 중 PC 및 노트북은 공유기를 통해 웹사이트에 접속하는 정상 범주의 동작을 수행하고 있으므로 해당 동작에 대해서는 로그를 생성하지 않으며, 스마트폰 및 외부 단말에서 공유기로 접속하여, 공유기의 IP(DST)로 접속을 시도하는 패킷이 생성될 수 있다. 실시예에서, 공유기로 접속하는 패킷이 생성되면, 공유기는 해당 패킷에 대해서 네트워크 접속 로그를 생성할 수 있다.

[0046] 도 2(c)의 실시예에 따르면, 사용자 단말 중 PC 및 노트북은 공유기를 통해 웹사이트에 접속하는 정상 범주의 동작을 수행하고 있으므로 해당 동작에 대해서는 로그를 생성하지 않으며, 공유기에서 내부 서버나 외부 서버로 접속하는 경우에 대해서 공유기는 네트워크 접속 로그를 생성할 수 있다.

[0047] 실시예에서, 일반적인 공유기는 메모리 및 스펙 등을 고려하면, 모든 패킷 정보를 저장하기 어렵다. 따라서, 로그의 최소화를 위해 외부에서 접근하는 패킷 및 공유기에서 외부로 접속하는 패킷에 대해서 주요 정보만을 로

그로 생성할 수 있다.

[0049] 다시, 도 1을 참조하면, 단계(106)에서 공유기는, 생성된 로그를 공유기 보안 침해 점검 서버로 전송할 수 있다.

[0050] 실시예에서, 공유기는 미리 정해진 주기로, 또는 실시간으로 대량의 접속 로그를 전송할 수 있다. 예를 들어, FTP(File transfer protocol)을 포함하여 다양한 방식으로 전송할 수 있다.

[0051] 단계(107)에서 공유기 보안 침해 점검 서버는, 수신된 로그를 분석할 수 있다.

[0052] 실시예에서, 공유기에서 외부 서버로 접속 시도하는 경우에 대한 로그에 대해서 외부 IP를 분석하여 비정상 IP인 경우, 공유기가 침해되었다고 판단할 수 있다. 이에, 단계(102)를 통해 등록된 정상 IP 정보를 이용할 수 있다. 공유기에서 외부 서버로 접속하는 IP는 DHCP, NTP, 프로비저닝 서버 등으로 미리 정의되어 있다.

[0053] 또한, 공유기에서 받은 로그를 분석하여 공격 IP 및 침해 공유기를 검출할 수 있다. 비정상 IP로 분류된 접속 IP에 대해서는 다양한 방법으로 침해 분석을 진행할 수 있다. 예를 들어, 이상 외부 IP, 예컨대 해외 IP, 접속 빈도 및 동일 IP의 접속 등에 대해서 분석을 진행할 수 있다.

[0054] 실시예에서, 통신사 서버의 경우, 수 많은 공유기를 사용하기 때문에, 수집된 로그 정보에서 동일한 외부 IP를 검출하는 경우, 공격 시도 IP로 판단할 수 있다. 공유기가 디폴트로 사용하는 외부 IP가 아닌 경우, 공유기가 이미 침해되었다고 판단할 수 있다.

[0055] 단계(108)에서 공유기 보안 침해 점검 서버는 분석 결과를 관리 장치로 전송하고, 관리 장치는 분석 결과가 공유기 침해로 판단된 경우 단계(109)에서 공유기로 조치를 취할 수 있다.

[0056] 일측에 따르면, 공유기를 초기화하거나, 펌웨어(FW, Firmware) 업그레이드 등의 조치를 취할 수 있다.

[0058] 도 3은 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 서버를 통해 수행되는 공유기 보안 침해 점검 방법을 설명하기 위한 흐름도이다.

[0059] 단계(310)에서 공유기 보안 침해 점검 서버는, 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록한다.

[0060] 실시예에서, 프로비저닝 서버, 업그레이드 서버, 단말 관리 서버 등 공유기에 정상적으로 접속 가능한 서버의 IP에 대해서 등록하여, 이후 공유기 침해 점검 시 정상 및 비정상 분류 기준으로 이용될 수 있도록 한다.

[0061] 단계(320)에서, 공유기 보안 침해 점검 서버는 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신한다.

[0062] 실시예에서, 공유기에서 NAT나 포워딩 패킷에 대해서는 로그를 생성하지 않고, 공유기의 IP(DST)로 접속을 시도하는 패킷 및 공유기의 IP(SRC)를 이용하여 타 서버로 접속을 시도하는 패킷에 대해서 로그를 생성할 수 있다.

[0063] 예컨대, PC, 노트북이나 스마트폰 등 사용자 단말로 공유기를 통해 네트워크를 이용하여 웹사이트에 접속하는 패킷에 대해서는 로그를 생성하지 않을 수 있다. 공유기로 접속하는 패킷이 생성되면, 공유기는 해당 패킷에 대해서 네트워크 접속 로그를 생성하고, 공유기에서 내부 서버나 외부 서버로 접속하는 패킷에 대해서 공유기는 네트워크 접속 로그를 생성할 수 있다.

[0064] 단계(330)에서, 공유기 보안 침해 점검 서버는 정상 IP 정보를 이용하여 상기 수신된 로그를 분석한다.

[0065] 실시예에서, 공유기에서 외부 서버로 접속하는 IP는 DHCP, NTP, 프로비저닝 서버 등으로 미리 정의되어 있으므로, 공유기에서 외부 서버로 접속 시도하는 경우에 대한 로그에 대해서 외부 IP를 분석하여 정상 IP에 속하지 않는 비정상 IP인 경우, 분석을 통해 공유기가 침해되었다고 판단할 수 있다.

[0066] 비정상 IP로 분류된 접속 IP에 대해서는 다양한 방법으로 침해 분석을 진행할 수 있다. 예를 들어, 이상 외부 IP, 예컨대 해외 IP, 접속 빈도 및 동일 IP의 접속 등에 대해서 분석을 진행할 수 있다.

[0067] 실시예에서, 통신사 서버의 경우, 수 많은 공유기를 사용하기 때문에, 수집된 로그 정보에서 동일한 외부 IP를 검출하는 경우, 공격 시도 IP로 판단할 수 있다. 공유기가 디폴트로 사용하는 외부 IP가 아닌 경우, 공유기가 이미 침해되었다고 판단할 수 있다.

[0068] 단계(340)에서, 공유기 보안 침해 점검 서버는 로그의 분석 결과를 보안 침해 관리 장치로 전송한다.

[0069] 실시예에서, 관리 장치는 분석 결과가 공유기 침해로 판단된 경우 공유기로 조치를 취할 수 있다. 예를 들어, 공유기를 초기화하거나, 펌웨어(FW, Firmware) 업그레이드 등의 조치를 취할 수 있다.

[0071] 도 4는 본 발명의 일실시예에 있어서, 공유기 보안 침해 점검 방법을 수행하는 공유기 보안 침해 점검 서버의 구성을 설명하기 위한 블록도이다. 실시예에 따른 공유기 보안 침해 점검 서버(400)는, 등록부(410), 수신부(420), 분석부(430) 및 전송부(440)를 포함한다.

[0072] 등록부(410)는, 보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록한다.

[0073] 실시예에서, 프로비저닝 서버, 업그레이드 서버, 단말 관리 서버 등 공유기에 정상적으로 접속 가능한 서버의 IP에 대해서 등록하여, 이후 공유기 침해 점검 시 정상 및 비정상 분류 기준으로 이용될 수 있도록 한다.

[0074] 수신부(420)는 공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신한다.

[0075] 실시예에서, 공유기에서 NAT나 포워딩 패킷에 대해서는 로그를 생성하지 않으며, 공유기의 IP(DST)로 접속을 시도하는 패킷 및 공유기의 IP(SRC)를 이용하여 타 서버로 접속을 시도하는 패킷에 대해서 로그를 생성할 수 있다.

[0076] 예컨대, PC, 노트북이나 스마트폰 등 사용자 단말로 공유기를 통해 네트워크를 이용하여 웹사이트에 접속하는 패킷에 대해서는 로그를 생성하지 않을 수 있다. 공유기로 접속하는 패킷이 생성되면, 공유기는 해당 패킷에 대해서 네트워크 접속 로그를 생성하고, 공유기에서 내부 서버나 외부 서버로 접속하는 패킷에 대해서 공유기는 네트워크 접속 로그를 생성할 수 있다.

[0077] 분석부(430)는 정상 IP 정보를 이용하여 수신된 로그를 분석한다.

[0078] 실시예에서, 공유기에서 외부 서버로 접속하는 IP는 DHCP, NTP, 프로비저닝 서버 등으로 미리 정의되어 있으므로, 공유기에서 외부 서버로 접속 시도하는 경우에 대한 로그에 대해서 외부 IP를 분석하여 정상 IP에 속하지 않는 비정상 IP인 경우, 분석을 통해 공유기가 침해되었다고 판단할 수 있다.

[0079] 비정상 IP로 분류된 접속 IP에 대해서는 다양한 방법으로 침해 분석을 진행할 수 있다. 예를 들어, 이상 외부 IP, 예컨대 해외 IP, 접속 빈도 및 동일 IP의 접속 등에 대해서 분석을 진행할 수 있다.

[0080] 실시예에서, 통신사 서버의 경우, 수 많은 공유기를 사용하기 때문에, 수집된 로그 정보에서 동일한 외부 IP를 검출하는 경우, 공격 시도 IP로 판단할 수 있다. 공유기가 디폴트로 사용하는 외부 IP가 아닌 경우, 공유기가 이미 침해되었다고 판단할 수 있다.

[0081] 전송부(440)는 로그의 분석 결과를 보안 침해 관리 장치로 전송한다.

[0082] 실시예에서, 관리 장치는 분석 결과가 공유기 침해로 판단된 경우 공유기로 조치를 취할 수 있다. 예를 들어, 공유기를 초기화하거나, 펌웨어(FW, Firmware) 업그레이드 등의 조치를 취할 수 있다.

[0084] 본 발명의 실시예를 통해서 일반적으로 보안에 취약한 공유기에 대해서 공유기 접속 로그를 분석함으로써 공유기 보안의 침해 여부를 판단하기 위한 공유기 보안 침해 점검 방법 및 그 시스템을 제공할 수 있다.

[0085] 또한, 공유기 공격에 대해 사전에 감지하고, 이미 침해된 공유기 정보를 제공함으로써 공유기의 보안을 강화하고, 보다 안전한 인터넷 사용이 가능하다.

[0087] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic media), CD-ROM, DVD와 같은 광기록 매체(Optical media), 플롭티컬 디스크(Floptical disk)와 같은 자기-광 매체(Magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

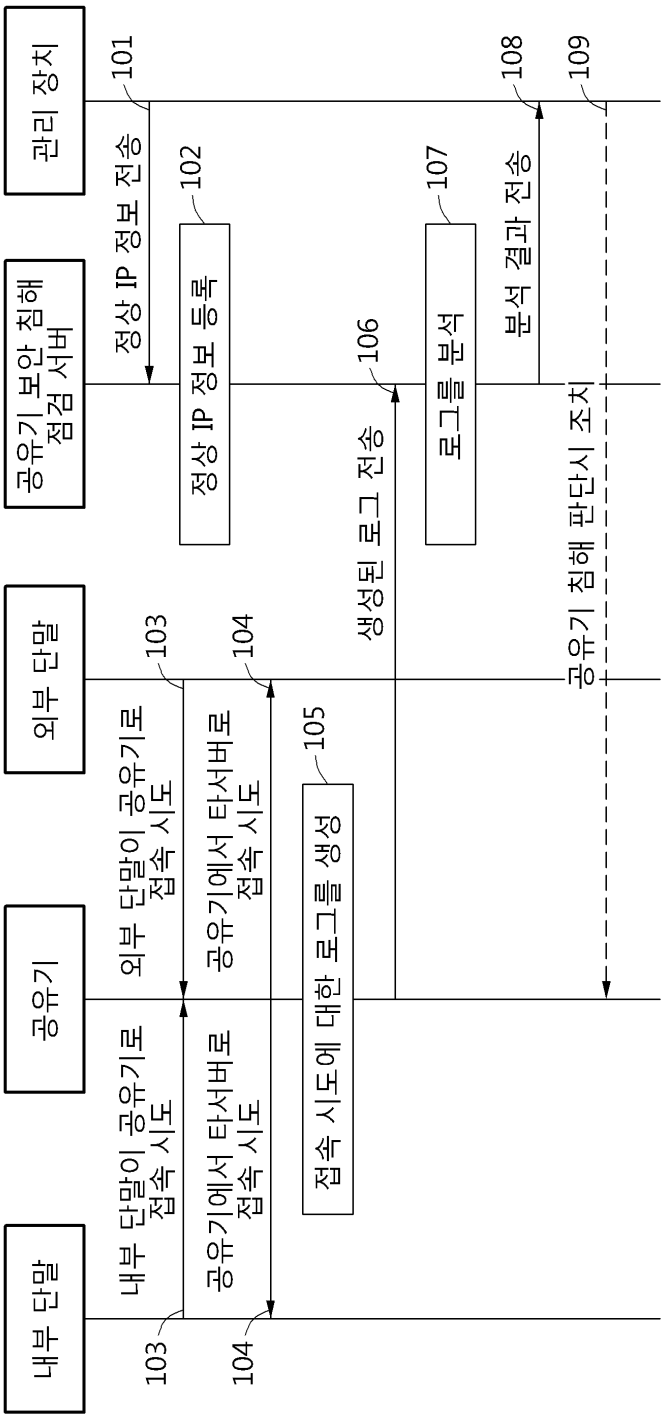
[0088] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태

로 결합 또는 조합되거나, 다른 구성요소 또는 균등한 것들에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

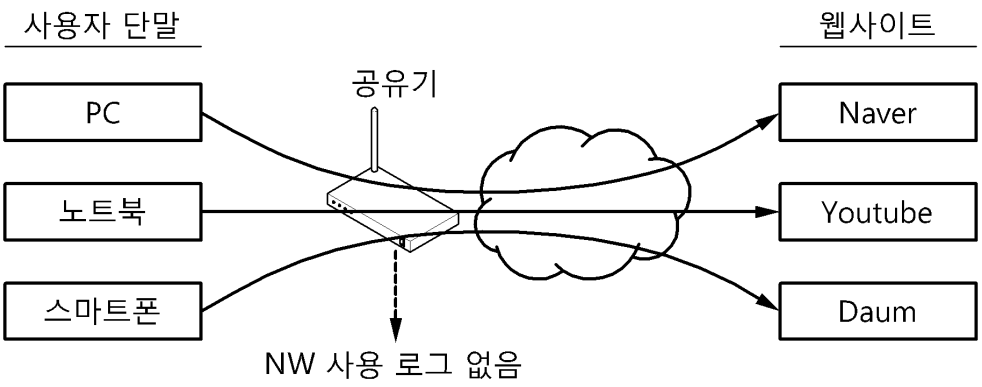
[0089] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

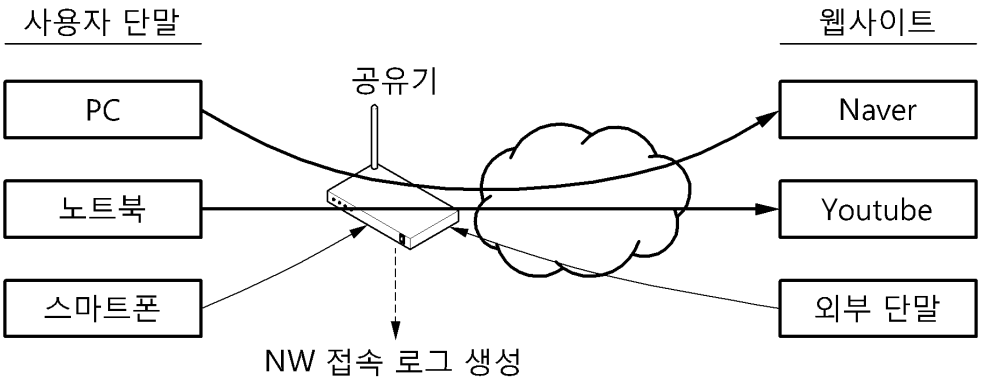
도면1



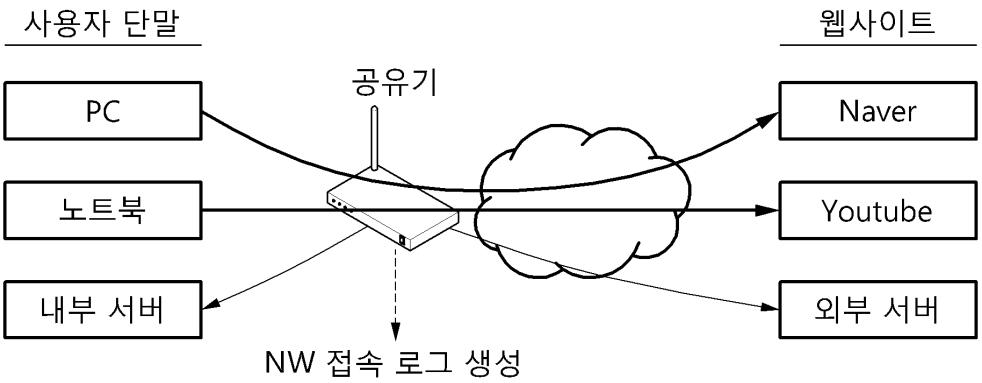
도면2


사용자 단말
웹사이트
공유기
PC
노트북
스마트폰
Naver
Youtube
Daum
NW 사용 로그 없음

(a)

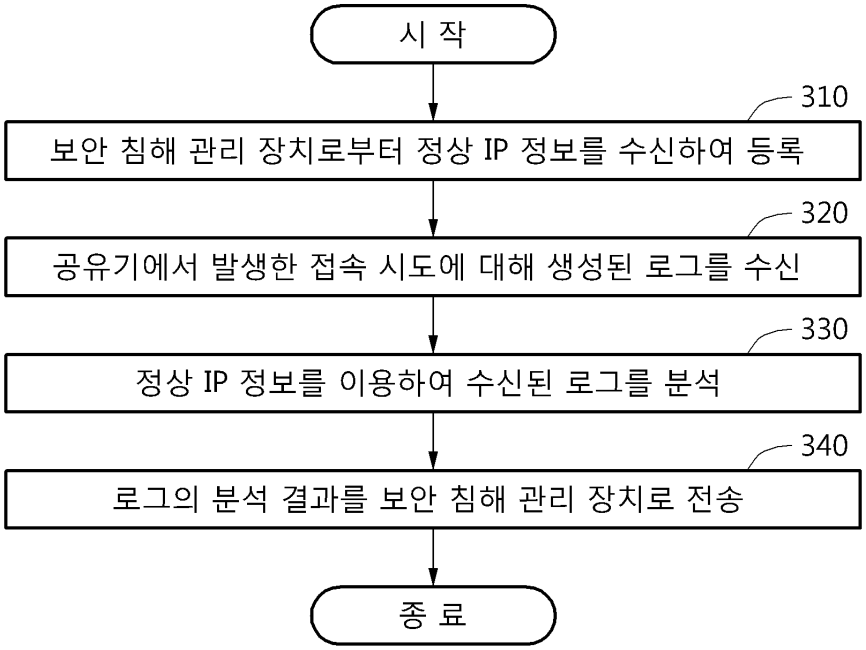

사용자 단말
웹사이트
공유기
PC
노트북
스마트폰
Naver
Youtube
외부 단말
NW 접속 로그 생성

(b)

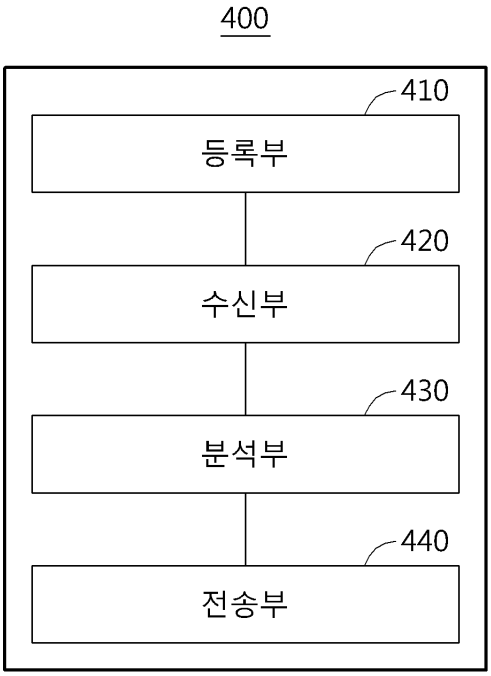

사용자 단말
웹사이트
공유기
PC
노트북
내부 서버
Naver
Youtube
외부 서버
NW 접속 로그 생성

(c)

도면3


시 작
310
보안 침해 관리 장치로부터 정상 IP 정보를 수신하여 등록
320
공유기에서 발생한 접속 시도에 대해 생성된 로그를 수신
330
정상 IP 정보를 이용하여 수신된 로그를 분석
340
로그의 분석 결과를 보안 침해 관리 장치로 전송
종 료

도면4


400
410
등록부
420
수신부
430
분석부
440
전송부