|  |
| --- |
| **오픈소스 방화벽 시스템 분석 및 취약점 사례연구**  **요 약**  오픈 소스 방화벽 시스템 중 하나인 pfSense에 대해 알아보고, 다른 방화벽 소프트웨어와 비교함으로써 사이버 위협으로부터 효과적인 네트워크 및 데이터 보호에 필수적인 기능을 더 깊이 이해하며, 취약성 사례를 통해 시스템의 잠재적인 약점을 식별하고 이를 완화하기 위한 방법을 모색한다. |

**1. 연구 배경 및 소개**

**1.1 연구 배경**

방화벽은 사이버 위협으로부터 네트워크와 데이터를 보호하는 데 도움이 되는 모든 네트워크 보안 전략의 필수적인 부분으로 오픈 소스 방화벽 시스템은 유연성, 비용 효율성 및 커뮤니티 지원 등으로 큰 인기를 얻고 있다. 그에 반해, 오픈 소스 방화벽 시스템에 대한 실제 공격에 대한 취약성 분석 및 사례 연구 등이 부족하기 때문에 본 연구는 오픈 소스 방화벽 시스템 중 가장 널리 사용되는 pfSense를 중심으로 오픈 소스 방화벽 시스템의 취약점을 분석하는 것을 목표로 한다. 또한, pfSense 이외의 다른 오픈 소스 및 상용 방화벽 시스템들과 비교하여 pfSense의 강점과 약점에 대한 포괄적인 내용을 연구한다.

**1.2 연구 목적**

오픈 소스 방화벽 시스템을 분석하는 목적은 존재할 수 있는 잠재적 취약점뿐만 아니라 강점과 약점을 식별하여 개선점 보완 및 식별된 위험을 완화함에 있다. 이번 연구는 오픈 소스 방화벽 시스템 중 하나인 pfSense를 기준으로 하여 해당 기능과 사례를 알아보고, 그 외의 오픈 소스 방화벽 시스템들과 비교·분석하여 특정 상황에 대한 가장 적합한 시스템을 찾아보고 결정하는 데 있다.

전반적인 연구 목표는 시스템의 보안 및 안정성을 향상하는 것으로, 잠재적 취약성을 식별하고 적절한 보안 조치를 구현함으로써 오픈 소스 방화벽 시스템이 네트워크와 데이터를 보호하기 위한 안전하고 효과적인 역할을 수행하는 것을 인지함에 있다.

**1.3 오픈 소스 방화벽의 정의**

오픈 소스 방화벽이란 미리 정해진 보안 규칙에 따라 들어오고 나가는 네트워크 트래픽을 감시하고 제어하는 ​​네트워크 보안 시스템인 방화벽을 오픈 소스 소프트웨어를 사용하여 구축한 시스템이다. 오픈 소스 방화벽은 사용자가 특정 보안 요구 사항에 맞게 지정하고 수정할 수 있으며 일반적으로 Linux 운영 체제를 사용하며 패킷 필터링, 침입 탐지 및 방지 등과 같은 다양한 기능을 제공한다.

**1.4 오픈 소스 소프트웨어와 독점 소프트웨어**

오픈 소스 소프트웨어와 독점 소프트웨어는 라이센스 및 개발 모델이 다른 유형의 소프트웨어다. 오픈 소스 소프트웨어는 사용자가 소스 코드를 보고 수정하여 배포할 수 있는 라이선스에 따라 배포된다. 반면, 독점 소프트웨어는 소스 코드에 대한 액세스를 제한하고 소프트웨어를 수정하거나 재배포할 수 있는 권한을 제한하여 배포된다.

오픈 소스 소프트웨어와 독점 소프트웨어의 주요 차이점 중 하나는 비용이다. 오픈 소스 소프트웨어는 무료로 사용할 수 있는 반면, 독점 소프트웨어는 라이센스 비용이 필요하다. 따라서, 한정적인 예산을 가진 기업이나 개인에게는 오픈 소스 소프트웨어의 사용이 훨씬 효율적이다.

또 다른 차이점은 유지보수이다. 독점 소프트웨어는 일반적으로 제품에 대한 기술 지원 및 유지 관리 서비스를 제공하는 반면, 오픈 소스 소프트웨어는 개발자 및 사용자 커뮤니티에서 제공하는 경우가 대부분으로 독점 소프트웨어에 비해 지원에 대한 제한이나 응답 시간의 지연 등이 발생할 수 있다.

마지막으로, 사용자의 특정 요구에 대한 차이가 있다. 오픈 소스 소프트웨어는 특정 요구 사항을 충족하도록 수정 및 사용자 정의할 수 있는 반면, 독점 소프트웨어는 종종 사용자 정의 기능이 제한된다.

결론적으로, 오픈 소스 소프트웨어와 독점 소프트웨어 간의 선택은 비용, 지원, 보안 및 유연성을 비롯한 다양한 요소에 따라 달라지는데, 두 가지 유형의 소프트웨어 모두 장단점이 있으며 결정은 해당 소비자의 요청 사항에 따라 달라질 수 있다.

**2. pfSense 방화벽 시스템 개요**

**2.1 특징 및 기능**

pfSense는 기업, 교육 기관, 정부 및 홈 네트워크에서 가장 널리 사용되는 오픈 소스 방화벽 시스템으로, 사이버 위협으로부터 네트워크와 데이터를 보호하는 데 도움이 되는 다양한 기능을 제공한다.

**2.1.1 패킷 필터링(Packet Filtering)**

패킷 필터링은 pfSense의 핵심 기능으로 관리자가 트래픽 흐름을 제어하고 무단 액세스를 방지하기 위한 규칙을 정의할 수 있도록 하여 네트워크 보호에 집중하는데, 특히 방화벽을 통과하는 패킷을 필터링하여 네트워크를 보호한다.

또한, 네트워크를 통해 전송되는 패킷의 헤더를 분석하고, 미리 정의된 규칙 집합에 따라 필터링하는 방식으로 작동하기 때문에, 이러한 기능을 통해 사용자는 소스 및 대상 IP 주소, 포트 번호, 프로토콜 및 기타 요소를 기반으로 규칙을 만들 수 있다.

나아가, 여러 인터페이스를 지원하기 때문에 각 인터페이스에 대한 방화벽 규칙을 개별적으로 생성할 수 있고, 이를 통해 관리자는 서로 다른 네트워크 간의 트래픽 흐름을 제어하고 각 네트워크에 서로 다른 규칙을 적용할 수 있다.

**2.1.2 로드 밸런싱(Load Balancing)**

로드 밸런싱은 최적의 성능과 가용성을 보장하기 위해 여러 인터넷 연결에 트래픽을 분산시켜 네트워크를 보호하는 방식으로 가동 중지 시간을 줄이고 네트워크 가용성을 개선하며 네트워크 리소스를 효율적으로 활용하는 데 도움이 된다.

특히, pfSense는 라운드 로빈, 최소 연결 및 고정 연결과 같은 트래픽 분산을 위한 여러 알고리즘을 지원하는데, 이러한 알고리즘을 통해 네트워크 관리자는 특정 요구 사항과 요구 사항에 따라 여러 인터넷 연결에 트래픽이 분산되는 방식을 제어할 수 있다.

로드 밸런싱이 활성화되면, pfSense는 여러 ISP를 포함한 여러 인터넷 연결에 트래픽을 분산하여 네트워크 트래픽을 효율적이고 효과적으로 관리할 수 있고, 이렇게 하면 연결 중 하나가 실패하거나 다운타임이 발생하는 경우에도, 네트워크 리소스에 더 나은 성능과 가용성을 제공할 수 있다.

**2.1.3 침입 탐지 및 방지(IDS/IPS)**

IDS/IPS(침입 탐지 및 방지 시스템)는 사이버 위협으로부터 네트워크를 보호하는 기능으로, 이를 통해 시스템은 악의적인 트래픽을 탐지 및 방지하고 다양한 유형의 사이버 공격으로부터 보호할 수 있다.

IDS(Intrusion Detection System) 기능은 네트워크 트래픽을 모니터링하고 알려진 공격 서명 세트 또는 악의적인 활동을 나타내는 동작 패턴과 비교하는데, 공격 서명이 감지되면 IDS는 경고를 생성하고 트래픽을 차단하거나 관리자에게 이메일 알림을 보내는 등 적절한 조치를 취한다.

IPS(Intrusion Prevention System) 기능은 악의적인 트래픽을 탐지할 뿐만 아니라, 실시간으로 네트워크 트래픽을 모니터링하고 알려진 공격 서명과 일치하는 트래픽을 능동적으로 차단할 수 있다. 이를 통해 제로 데이 공격 또는 이전에 알려지지 않은 취약점을 악용하는 공격으로부터 네트워크를 보호할 수 있다.

pfSense는 이러한 IDS와 IPS 모두 구성이 가능하며, 관리자가 네트워크의 특정 요구 사항에 맞게 규칙과 정책을 사용자 정의할 수 있다.

**2.1.4 네트워크 주소 변환(NAT; Network Address Translation)**

NAT(Network Address Translation)는 개인 IP 주소를 공용 IP 주소에 매핑하여 네트워크를 보호하는 방화벽 시스템으로 사설 네트워크 내 여러 장치가 단일 공용 IP 주소를 공유할 수 있도록 하는 데 사용된다. 개인 네트워크의 장치가 인터넷 액세스 요청을 보내면 요청은 pfSense의 NAT 기능에 의해 변환되고, 인터넷의 응답은 NAT 기능으로 다시 전송된 다음, 개인 네트워크의 적절한 장치로 라우팅 된다.

또한, 외부 장치가 특정 포트에서 들어오는 트래픽을 해당 장치로 전달하여 사설 네트워크의 특정 장치에 연결할 수 있도록 하는 포트 포워딩도 지원하는데, 이러한 기능은 일반적으로 개인 장치에서 실행되는 웹 서버, FTP 서버 또는 기타 네트워크 응용 프로그램과 같은 서비스에 대한 외부 액세스를 허용하는 데 사용된다.

또한, 1:1 NAT를 지원함으로써 관리자가 공용 IP 주소를 네트워크의 특정 개인 IP 주소에 매핑할 수 있고, 이것은 일반적으로 네트워크의 특정 장치가 외부 액세스를 위해 공용 IP 주소를 요구하는 시나리오에서 사용된다.

**2.1.5 서비스 품질(QoS; Quality of Service)**

서비스 품질(QoS)은 관리자가 네트워크 트래픽의 우선순위를 지정하고 관리하여 중요한 응용 프로그램에 대한 최적의 성능을 보장할 수 있도록 하며, 네트워크 정체를 방지하고 다양한 유형의 네트워크 트래픽 간에 대역폭이 공정하게 할당되도록 한다.

주요 기능으로는 관리자가 특정 규칙 및 우선순위에 따라 대역폭을 할당할 수 있는 트래픽 셰이핑(Traffic Shaping), 특정 유형의 트래픽이 사용할 수 있는 대역폭의 양 제한 및 우선순위 지정, 실시간 모니터링 기능 등이 있으며, 이를 통해 네트워크 문제를 신속하게 식별하고 해결할 수 있도록 한다.

**3. pfSense와 다른 방화벽 솔루션 비교**

**3.1 다른 오픈 소스 방화벽 시스템**

**3.1.1 OPNsense**

OPNsense는 FreeBSD 운영 체제를 기반으로 하는 무료 오픈 소스 방화벽 시스템으로, 소규모 및 대규모 네트워크 모두에 고급 보안 기능을 제공하도록 설계되었다. OPNsense는 사용자 정의 및 구성이 가능하여 광범위한 네트워크 환경에 적합하다. 또한, OpenVPN 및 IPsec을 비롯한 다양한 VPN 프로토콜을 지원하여 네트워크 외부에서 연결하는 사용자를 위한 원격 액세스 및 보안 연결을 허용하고, 웹 프록시 기능이 포함되어 있어 관리자가 웹 트래픽을 제어 및 필터링하고 SSL 검사와 같은 고급 보안 기능을 사용할 수 있도록 한다.

**3.1.2 Smoothwall**

Smoothwall은 중소 규모 네트워크에 고급 보안 기능을 제공하도록 설계된 오픈 소스 방화벽 시스템으로, 각 패킷의 연결 상태를 기반으로 네트워크 트래픽을 모니터링하고 필터링할 수 있는 상태 저장 패킷 검사 엔진이 포함되어 있으며, NAT를 지원하여 관리자가 내부 IP 주소를 외부 IP 주소에 매핑하고 외부 소스에서 네트워크에 대한 액세스를 제어할 수 있다. 또한, 콘텐츠 필터링 기능이 포함되어 있어 관리자가 특정 웹사이트에 대한 액세스를 차단하고 키워드 및 카테고리와 같은 다양한 기준에 따라 콘텐츠를 필터링할 수 있다.

**3.1.3 FirewallD**

FirewallD는 Linux 기반 시스템을 위한 오픈 소스 방화벽 관리 도구로, 방화벽 규칙을 구성하고 관리하기 위한 사용자에게 친숙한 인터페이스를 제공한다. 주요 기능은 네트워크 인터페이스를 영역으로 구성하고 미리 구성된 방화벽 규칙을 각 영역에 적용하여 다양한 네트워크 구성에 대한 방화벽 규칙을 보다 쉽게 ​​관리하고 구성할 수 있고, 방화벽 서비스를 다시 시작하지 않고도 즉시 방화벽 규칙을 추가 및 제거할 수 있다. 또한, 로깅 및 경고 기능을 제공하여 방화벽 활동을 모니터링하고 특정 이벤트에 대한 경고를 생성할 수 있고 IPv4 및 IPv6 네트워크 프로토콜을 모두 지원한다.

**3.2 pfSense만의 장** **·단점**

**3.2.1 장점**

첫째, 비기술적인 사용자도 쉽게 사용하고 탐색할 수 있는 매우 사용자 친화적인 웹 기반 인터페이스를 제공한다.

둘째, 패킷 필터링, 네트워크 주소 변환(NAT), VPN 지원, 로드 밸런싱, 트래픽 셰이핑, 침입 탐지 및 방지를 포함한 다양한 기능을 제공하는 다재다능하고 강력한 방화벽 솔루션이다.

셋째, 애드온 패키지를 사용하여 쉽게 사용자 지정 및 확장할 수 있으므로 광범위한 네트워크 환경 및 보안 요구 사항에 적응할 수 있는 유연함이 있다.

넷째, 사용자 및 개발자로 구성된 대규모의 활성 커뮤니티가 있어 풍부한 지식 및 지원 리소스에 대한 액세스를 제공한다.

**3.2.2 단점**

첫째, 리소스 집약적이어서 다른 오픈 소스 방화벽 시스템보다 더 강력한 하드웨어가 필요하여 요구 사항이 꽤 까다롭다.

둘째, 사용자에게 친숙하지만, 특히 네트워킹 및 보안 개념에 익숙하지 않은 사용자의 경우 다른 오픈 소스 방화벽 시스템보다 설정 및 구성이 더 복잡할 수 있다.

셋째, 사용할 수 있는 커뮤니티 리소스가 많지만, pfSense에 대한 공식 문서가 제한되거나 오래되어 문제를 해결하거나 새로운 기능에 대해 알아보기가 더 어려울 수 있다.

넷째, 오픈 소스지만 GPL과 같은 다른 오픈 소스 라이선스와는 다른 요구 사항 및 제한 사항이 있을 수 있는 BSD 라이선스에 따라 라이선스가 부여된다.

**3.3 시장 점유율 및 추이**

오픈 소스 방화벽 시스템 시장은 저렴하고 유연한 네트워크 보안 솔루션에 대한 수요가 증가함에 따라 최근 꾸준히 성장하고 있으며, 2020년부터 2027년까지 약 16%의 연평균 성장률로 성장할 것으로 예상된다.

가장 인기 있는 오픈 소스 방화벽 시스템 중 하나는 pfSense이며 고급 보안 기능과 사용자 친화적인 인터페이스로 상당한 시장 점유율을 얻고 있다. 다른 오픈 소스 방화벽 시스템으로는 OPNsense, iptables, FirewallD 및 Untangle 등이 있다.

오픈 소스 방화벽 시스템 시장의 한 가지 추세는 클라우드 기반 솔루션(PaaS)의 채택이 증가하고 있다는 것이다. 많은 조직에서 인프라를 클라우드로 이동하고 있으며 이로 인해 클라우드 기반 보안 솔루션이 필요하게 되었고, pfSense 및 OPNsense와 같은 오픈 소스 방화벽 시스템은 이런 시스템을 쉽게 배포하고 관리할 수 있도록 함으로써 시장 점유율을 높이고 있다.

전반적으로 오픈 소스 방화벽 시스템 시장은 저렴하고 유연한 네트워크 보안 솔루션에 대한 수요 증가로 인해 향후 몇 년 동안 계속 성장할 것으로 예상되며, 클라우드 기반 솔루션을 향한 추세와 자동화 및 사용 편의성에 대한 초점은 네트워크 보안뿐만 아니라 넓은 분야에서 시장을 형성할 것이다.

**4. 보안 취약성 조사**

본 연구에서는 오픈 소스 방화벽 시스템에 영향을 미칠 수 있는 취약점을 조사하여 분석할 것이며, 이를 통해 오픈 소스 방화벽 시스템에 영향을 미칠 수 있는 가장 심각한 보안 취약점을 식별 및 평가하고 이러한 취약점을 완화하기 위한 권장 사항을 제공하는 것을 목표로 한다. 이 조사에는 잠재적인 약점을 식별하기 위한 테스트 및 실험 등 기본 구성 및 시스템 아키텍처에 대한 철저한 분석을 포함할 것이며, 궁극적으로 오픈 소스 방화벽 시스템의 전반적인 보안과 복원력을 개선하고 조직이 잠재적인 위협으로부터 네트워크와 데이터를 보호할 수 있도록 해답을 찾아보려 한다. 취약점은 다음과 같다.

* Denial of Service
* SQL Injection
* Buffer Overflow
* Cross Site Scripting(XSS)
* Improper Configuration
* Outdated Software
* Weak Passwords

**5. 향후 일정**

****

**6. 결론 및 기대효과**

이번 연구는 크게 세 가지 기대효과를 얻을 수 있다.

첫째, 이번 연구는 오픈 소스 방화벽 시스템, 특히 pfSense에 존재하는 보안 취약성에 대한 포괄적인 이해를 제공할 것이다. 특히, 시스템에서 발견된 취약점에 대한 실제 공격 및 사례 연구를 통하여 근본 원인을 발견하고, 나아가 취약점을 완화할 수 있는 방법에 대한 통찰력을 제공하고 향후 유사한 공격을 방지하는 데 도움이 되도록 할 것이다.

둘째, 이번 연구를 통해 pfSense와 다른 오픈 소스 및 상용 방화벽 시스템을 비교하여 각각의 시스템에 대한 강점과 약점의 포괄적인 개요를 제공하고, 네트워크 관리자와 보안 담당자가 방화벽 시스템을 관리할 때 정책 결정에 있어 도움이 되도록 할 것이다.

마지막으로, 본 연구는 네트워크의 전반적인 보안 인식에 긍정적인 영향을 미칠 것이며, 오픈 소스 방화벽 시스템의 취약점을 식별함으로써, 보다 안전한 방화벽 시스템의 개발을 가능하게 하고 네트워크의 전반적인 보안을 향상할 것이다.

전반적으로, 오픈 소스 방화벽 시스템 및 취약성 사례 연구 분석은 네트워크 보안 개선에 초점이 맞춰져 있으며, 이 연구를 통해 네트워크 관리자와 보안 담당자에게 사이버 위협으로부터 네트워크와 데이터를 보호하는 데 필요한 지식과 도구를 제공할 것이다.

**6. 참고문헌**

[1] Market Research Future, 2020년 7월, https://www.marketresearchfuture.com/press-release/open-source-intelligence-market