컴퓨터 보안

- 그림1

보안 시스템을 구성하기 위해서는 기업 또는 조직의 보안 정책과 요구사항에 맞게 여러 보안 기술과 솔루션을 조합하여 사용해야 합니다. 따라서 이 경우, 그림에서 나타난 요소들을 이용하여 적절한 보안 시스템을 구성해야 합니다.

여러 보안 시스템 중에서, 그림에서 나타난 요소들을 이용하여 구성할 수 있는 보안 시스템은 다음과 같습니다.

1. 인트라넷과 인터넷 간의 보안을 위해, 인터넷과 회사 내부를 연결하는 모든 경로에 방화벽을 설치합니다. 그림에서는 인터넷과 회사 내부 간에 2개의 경로가 있으므로, 각각의 경로에 방화벽을 설치합니다.
2. 인트라넷과 인터넷 간의 통신을 위해, VPN을 사용합니다. 그림에서는 SSL VPN을 사용하므로, SSL VPN 게이트웨이를 구성합니다. SSL VPN은 인터넷을 통해 안전하게 회사 내부 네트워크에 접속할 수 있도록 해줍니다.
3. 회사 내부에서 서버와 사용자 간의 통신을 안전하게 보호하기 위해, 내부 네트워크에서 사용하는 프로토콜 중 하나인 MPLS를 사용합니다. MPLS는 회사 내부에서 안전하게 데이터를 전송할 수 있도록 해줍니다.
4. 보안 관문 L3는 네트워크와 인터넷 간에 위치하고 있는 장치로, 이 장치를 사용하여 인터넷으로부터의 공격을 차단하고, 네트워크 내부로의 침입을 방지합니다.

위와 같이 다양한 보안 기술과 솔루션을 조합하여 보안 시스템을 구성하면, 기업 또는 조직의 보안을 보다 안전하게 보호할 수 있습니다.

1. 방화벽
   인터넷과 회사 내부를 연결하는 각각의 경로에 방화벽을 설치해야 합니다. 방화벽은 인터넷에서 들어오는 악성 코드나 해킹 시도 등을 차단하는 역할을 합니다. 또한, 내부 네트워크에서 인터넷으로 흐르는 트래픽을 모니터링하여 위협이나 이상행동을 탐지할 수 있습니다.
2. VPN
   회사 내부에서 외부로 접속하는 경우, SSL VPN을 사용하여 보안적으로 안전한 통신을

할 수 있습니다. SSL VPN 게이트웨이를 구성하여, 인터넷을 통해 안전하게 회사 내부 네트워크에 접속할 수 있도록 합니다.

3. MPLS
   MPLS는 회사 내부에서 안전하게 데이터를 전송할 수 있도록 하는 프로토콜입니다. 회사 내부에서 서버와 사용자 간의 통신을 안전하게 보호하기 위해, MPLS L3 스위치를 사용하여 내부 네트워크를 구성합니다.
4. 보안 관문 L3
   보안 관문 L3는 네트워크와 인터넷 간에 위치하고 있는 장치로, 인터넷으로부터의 공격을 차단하고, 내부로의 침입을 방지하는 역할을 합니다. 각각의 회선 구간 관문 L3 밑에는 방화벽이 설치되어 있으므로, 방화벽을 통과한 트래픽만 내부로 진입할 수 있습니다.

이러한 보안 시스템을 구성함으로써, 인터넷을 통해 들어오는 위협을 차단하고, 내부 네트워크를 안전하게 보호할 수 있습니다. 또한, SSL VPN을 통해 외부에서 안전하게 내부 네트워크에 접속할 수 있으며, MPLS를 사용하여 회사 내부에서 안전하게 데이터를 전송할 수 있습니다.

- 그림2
- OA, RA, FA Network는 일반적으로 다음과 같이 구성됩니다.
  - OA(Network A) : 외부 네트워크와 연결된 인터넷 게이트웨이, 방화벽, IDS/IPS 등의 보안장비가 설치된 네트워크입니다. OA(Network A)는 인터넷을 통해 접속할 수 있는 외부 사용자와 통신하며, 외부에서의 공격을 방어하고 내부 네트워크를 보호합니다.
  - RA(Network B) : 원격지 접속이 가능한 네트워크로서, VPN 연결을 통해 외부 접속자들이 접속합니다. RA(Network B)는 인터넷을 통해 외부에서 접속할 수 없으며, VPN 연결을 통해 인증된 사용자만 내부 네트워크에 접근할 수 있습니다.
  - FA(Network C) : 내부망으로서, OA(Network A)와 RA(Network B)에서의 보안장비를 통해 보호되고 있습니다. FA(Network C)는 인터넷과는 완전히 격리되어 있으며, 내부에서만 통신이 가능합니다.
- OA Network, RA Network, FA Network로 구성된 그림에서 보안 시스템을 구성하기 위해서는 다음과 같은 절차를 따를 수 있습니다:
  1. 위험 평가(Risk Assessment)를 수행합니다. OA Network, RA Network, FA Network 각각의 위험을 평가하고 보안 취약점을 식별합니다.

2. 보안 정책(Policy)을 개발합니다. 보안 정책은 위험 평가 결과를 기반으로 각 네트워크에 대한 보안 요구 사항을 정의합니다.
3. 네트워크 디자인(Network Design)을 수행합니다. 각 네트워크에 대한 보안 요구 사항을 충족시키기 위한 적절한 보안 제어들을 구현합니다.
4. 보안 제어(Control)을 구현합니다. 이 단계에서는 네트워크 디자인에서 결정한 보안 제어들을 구현합니다. 이는 방화벽(Firewall), 침입 탐지 시스템(Intrusion Detection System), 가상 사설망(Virtual Private Network) 등의 보안 기술을 사용하여 구현할 수 있습니다.
5. 보안 모니터링(Monitoring)과 보안 관리(Management)를 수행합니다. 이러한 단계에서는 네트워크에서 발생하는 보안 이벤트를 모니터링하고 보안 정책 및 보안 제어를 업데이트하여 보안 수준을 유지하고 개선합니다.
6. 교육과 교육 프로그램(Education and Training)을 제공합니다. 모든 사용자에게 보안 교육과 교육 프로그램을 제공하여 보안 정책을 이행하고 보안 사고를 방지합니다.

- 위와 같은 단계를 거쳐 OA Network, RA Network, FA Network 각각의 보안 요구 사항을 충족시키는 보안 시스템을 구성할 수 있습니다.
- 따라서, 이 세 가지 네트워크를 보호하기 위해서는 다음과 같은 보안시스템을 구성해야 합니다.

1. OA(Network A) 보안시스템
    - 인터넷 게이트웨이 : 외부 인터넷과 연결되는 포인트로서, 네트워크 트래픽을 제어하고 필터링합니다.
    - 방화벽 : 인터넷 게이트웨이와 내부 네트워크 간의 트래픽을 검사하여, 악성 트래픽을 차단합니다.
    - IDS/IPS : 외부에서의 침입을 탐지하고 차단하는 시스템으로서, 방화벽과 함께 연동하여 사용됩니다.
2. RA(Network B) 보안시스템
    - VPN Gateway : 외부 접속자들이 VPN 연결을 통해 접속할 수 있는 포인트입니다. VPN Gateway는 인증된 사용자만 내부 네트워크에 접근할 수 있도록 설정되어야 합니다.
    - 인증 서버 : VPN 접속자들의 인증 정보를 관리합니다. 인증 서버는 내부 네트워크와 동기화하여 인증 정보를 관리해야 합니다.
3. FA(Network C) 보안시스템

- 내부망 방화벽 : 내부 네트워크에서 발생하는 트래픽을 검사하여 악성 트래픽을 차단합니다.
- 내부망 IDS/IPS : 내부 네트워크