**발표자1 김민재**

**[첫 장]**

**카드사 네트워크 망 설계 및 보안 자동화 구축이라는 내용으로 발표를 하게 된 3팀 조장 김민재입니다.**

**[목 차]**

**프로젝트 목차는 다음과 같습니다. 프로젝트 팀 구성 및 역할, 개요, 수행 정차 및 방법, 수행 경과, 자체 평가 의견을 끝으로 발표를 마치겠습니다. 자체 평가 의견은 발표 시간상 관계로 발표하지 않도록 하겠습니다.**

**[훈련 내용과 연관성]**

**다음은 프로젝트 내용과 교육 훈련 내용과의 연관성입니다.교육 훈련 5가지 카테고리 중에 네트워크와 인프라 자동화 부분에 대한 내용을 바탕으로 프로젝트를 준비했습니다.**

**[팀 구성 및 역할]**

**먼저 프로젝트 팀 구성 및 역할입니다. 조장인 저와, 김현민님과 이창희님은 네트워크 구조를 설계하고 구현하는 역할을 담당하였습니다. 방민우님과 오수연님은 네트워크 자동화를 앤서블로 구현하는 역할을 담당하였습니다.**

**[프로젝트 주제 및 선정 배경, 기획 의도]**

**다음은 프로젝트 주제 및 선정 배경과 기획 의도입니다. 먼저 B 카드사는 전국에 ATM을 두고 금융 서비스를 운영하는 중이고 새로운 ATM 도입 시 보안 정책 자동화 시스템을 구축하고자 한다는 주제를 선정하였습니다.**

**그 이유가 되는 배경은 B카드사는 새로운 ATM 도입 시에 네트워킹 설정과 보안이 수작업으로 작업되었는데 수작업 시 발생하는 휴먼오류가 발생하고 있다는 것이고, 오류 발생 시에 다른 장비에 오류가 확산되고 오류에 대한 비용이 점차 증가하고 있음을 회사가 알게되었다는 배경입니다.**

**프로젝트 기획 의도는 학원에서 습득한 물리적 네트워킹 지식과 보안 기술을 활용하여 인프라를 구축해 그 인프라 환경에서 Ansible 기반 자동화를 통해 정책 누락 방지 및 효율성을 확보해보자는 취지로 기획 하였습니다.**

**[프로젝트 내용]**

**프로젝트 내용입니다.**

**문제 상황은 신규 ATM 장비 도입 시 보안 정책이 누락되어 포안 포트가 외부로 노출되어 보안이 취약한 상황입니다. 원인 분석을 해보니 기존 템플릿에 대한 신규 정책을 적용하지 않았었고 새로운 ATM 도입 시에 오류가 발생하였고 이로 인해 전국에 있는 수백 대 ATM이 외부로 접근이 가능하게 되고 또한 문제가 확산되어 본사와 지사간 네트워킹 보안에도 취약점이 발생할 수 있어 회사는 위험하다고 판단되어 해결책으로 Ansible 기반 표준 정책 템플릿을 설계하고 자동 배포를 하는 Playbook을 구성하는 것입니다.**

**[활용 장비 및 재료]**

**다음은 활용 장비 및 재료입니다.**

**저희 팀은 정책 자동화 도구로 엔서블을**

**가상 네트워크 시뮬레이션으로 PNETLab을**

**형상관리 및 코드 공유로 GitHub를**

**코드 공유, 일정 관리를 Notion으로 관리하였습니다.**

**[프로젝트 구조]**

**다음은 프로젝트 구조입니다. 이 사진은 전체 토폴로지 입니다.**

**[프로젝트 구조 - 영역]**

**구역으로 나누게 되면 좌상단에 보이는 장비가 전국에 설치된 ATM이고 이는 지역라우터에 연결됩니다. 지역 라우터는 또 통신사로 가정한 ISP들에 연결됩니다. ISP는 본사, 지사, 데이터센터를 연결한 라우터에 연결되고 이 라우터는 트래픽을 전달할 때 VPN을 활용하여 암호화 합니다. 데이터 센터에는 DMZ 구역을 설정하여 데이터 센터에서 활용하는 중요한 장비에 대한 보안을 강화하였습니다.**

**[프로젝트 구조 - 기술]**

**다음은 기술 영역으로 나눈 그림입니다. 검은색 외각선 영역은 라우팅 프로토콜에 대한 영역을 나타냅니다. 라우팅 프로토콜은 BGP, OSPF를 사용하였습니다. 본사, 지사, 데이터 센터를 연결하는 영역에는 IPSec Tunnel 모드를 사용하여 네트워크 계층의 보안을 강화하였습니다. 각각의 본사, 지사, 데이터센터에 설치된 ASA 방화벽에서 ACL을 통해 보안 정책을 설정하였습니다. DMZ 구역 안에있는 라우터에는 NAT를 설정하여 외부에서 사설 IP가 보이지 않도록 하였고 또한 이 라우터에도 ACL을 통해 보안 정책을 설정하였습니다. 게이트웨이 장애 발생 시에도 통신이 끊기지 않도록 하기 위해 아래 단에 HSRP를 사용하였습니다.**

**[프로젝트 활용방안 및 기대 효과]**

**프로젝트의 활용 방안으로 Ansible로 보안 정책을 자동 배포 함으로서 운영 효율성을 향상 시킬 수 있고**

**반복 업무를 자동화함으로서 서비스 가용성을 향상시킬 수 있습니다.**

**또한 네트워크 보안을 효율적으로 관리함으로서 컴플라이언스 리스크를 완화시킬 수 있습니다.**

**[프로젝트 수행 절차 및 방법]**

**[내 역할]**

**저는 네트워크 부분에서 HSRP, VPN, NAT, BGP를 담당.**

**발표자2 – 김현민**

**안녕하세요.**

**저는이번팀 프로젝트에서 BGP, 재분배(Redistribution), IPsec VPN, HSRP,Failover 기술을 적용하는 네트워크 파트를 담당했습니다.**

**먼저 전체 네트워크는 지사, 본사, 데이터센터를 포함한 Full-Mesh 구조로 구성하였습니다.**

**이렇게 구성한 이유는 고가용성 확보, 트래픽 부하 분산, 최단 경로 확보를 통해 지연 시간을 최소화하고, 장애 시 빠른 우회가 가능하도록 하기 위함입니다.**

**내부에는OSPF를 사용하고, 외부망과 연동되는 라우터에는 BGP를 적용했습니다.**

**지사, 본사, 데이터센터는 모두 AS 7로 통일하고, ISP1은 AS 107, ISP2는 AS 1009로 설정하여 BGP를 통한 외부 연동이 가능하게 구성했습니다.**

**이때 내부 OSPF 경로를 외부 BGP로 전달하고, 다시 외부 BGP 경로를 내부 OSPF로 유입시키기 위해 라우팅 재분배 기술을 적용했습니다.**

**이 과정에서 default-information originate 명령어를 통해 디폴트 경로도 광고하였고, 이를 통해 불필요한 경로 유입을 방지하고, 경로 루프 없이 안정적인 경로 설정이 가능했습니다.**

**게이트웨이1라우터와 게이트웨이2라우터에 각각 show ip bgp 명령어를 통해 ISP1과 ISP2의 경로가 모두 표시되는 것을 확인했습니다.**

**이는bgp와 내부 OSPF 경로가 외부 BGP로, 외부 BGP 경로가 다시 내부로 정상적으로 재분배되었다는 것을 의미합니다.**

**보안 측면에서는 지사, 본사, 데이터센터 간의 통신이 공용망을 통해 이루어지기 때문에, IPsec VPN 기술을 적용해 보안을 강화했습니다.**

**AES 암호화와 SHA 무결성 검증, 터널 모드를 통해 데이터의 기밀성과 안전한 전송을 보장했습니다.**

**이 사진은 지사 라우터에서 게이트웨이1라우터로 ipsec vpn 코맨드 적용이 잘 되었는지 와이어샤크로 캡처한 결과예시입니다.**

**133.0.0.1과 133.0.0.2 사이에 ISAKMP 패킷(Main Mode) 가 보이며 이는 Phase 1 키 교환,**

**이후 나타나는 Quick Mode는 Phase 2로, 암호화 터널 설정 완료를 의미합니다.**

**즉, 두 지점 간 IPsec 터널이 성공적으로 형성되었고, 보안이 확보된 상태로 데이터 통신이 가능하다는 것을 확인할 수 있었습니다.**

**또한 본사와 데이터센터내부에서 장애 대응을 위한 이중화 구성도 적용했습니다.**

**금융망처럼 안정성이 중요한 환경을 고려해 핵심 라우터에는 HSRP 기술을 적용하였습니다.**

**예를 들어, 본사에서는 라우터 3번을 Active, 4번을 Standby로 설정해서, 기본 통신은 3번을 통해 이루어지고, 장애 발생 시 자동으로 4번 라우터로 통신이 전환되도록 구성했습니다.**

**마지막으로 데이터센터의 ASA 방화벽에는 Failover 기술을 적용했습니다.**

**주 방화벽과 대기 방화벽 간에 세션 상태까지 동기화되도록 구성하여, 장애 발생 시에도 보안 제어가 끊기지 않고, 중단 없는 트래픽 흐름이 가능하도록 설계했습니다.**

**이것은 hsrp 코맨드 적용 결과물입니다 show standby brief 명령어를 통해 액티브스탠바이가 잘 적용됐음을 확인할 수 있습니다.**

**이러한 기술들을 통해 저희는 고가용성과 보안을 모두 고려한 안정적인 네트워크를 구현할 수 있었고, 실제로 다양한 장애 상황을 시뮬레이션했을 때에도 통신이 중단되지 않는 구조를 확인할 수 있었습니다.**

**감사합니다.**

**다음 asa방화벽 dmz 구성부분 부터는 이창희님이 발표하겠습니다.**

**발표자3 이창희**

**안녕하세요.**

**저는 이번 3조 팀 프로젝트에서 네트워크 부분을 맡고 있는 이창희 입니다.**

**저는 ASA 방화벽과 DMZ 구역 설계를 담당했습니다.**

**먼저 ASA 방화벽을 도입해 네트워크를 내부와 외부를 레벨 디자인으로 명확히 구분했습니다.**

**ASA 방화벽은 이 프로젝트에서 내부와 외부 네트워크를 명확히 분리하고,**

**보안 레벨 기반 정책으로 트래픽 흐름을 효과적으로 제어하며 외부로부터의 비인가 접근을 기본적으로 차단하기 위해 사용하였습니다.**

**(ASA 결과 화면)**

**이러한 세분화된 ACL과 결합해 본사·지사 등 필요한 트래픽만 허용하는 정밀한 접근 통제를 구현하였습니다.**

**특히 ASA 방화벽에서는 외부에서 들어오는 SSH 접속만 명확하게 차단하여, 외부에서의 SSH 공격 시도를 효과적으로 방어할 수 있도록 구성했습니다.**

**ASA 방화벽은 보안 레벨 외부에서 내부 방향의 모든 트래픽을 기본적으로 차단하는 원칙을 가지고 있어서**

**이 기본 차단 정책 위에 ACL을 오버레이 방식으로 덮어씌워서 세부적인 트래픽 제어를 구현했습니다.**

**외부에서 들어오는 SSH 트래픽은 본사, 지사, DR 센터 대역에서만 허용하고,**

**그 외 모든 SSH 트래픽은 차단하며, 나머지 IP 트래픽은 허용하도록 설계했습니다.**

**여기에 추가로 ACL을 적용해, 본사와 지사 네트워크에서 오는 TCP 트래픽만 세밀하게 허용하고,**

**그 외의 접근은 모두 차단함으로써 보안 레벨 기반 제어보다 더욱 정밀한 접근 통제와 최소 권한 원칙,**

**그리고 Zero Trust 보안 모델을 효과적으로 실현했습니다.**

**(DMZ 구현)**

**다음으로 DMZ 구역은 외부에 공개해야 하는 서버를 내부 네트워크와 분리해 배치함으로써, 카드사와 같은 금융 환경에서 고객 정보와 핵심 시스템을 외부 위협으로부터 효과적으로 보호할 수 있고, 필요한 서비스만 안전하게 외부에 제공하도록 설계 하였습니다.**

**먼저 DMZ에는 Static NAT를 적용해 내부 서버를 외부에서 안전하게 접근할 수 있도록 했습니다.**

**내부 IP와 외부 공인 IP를 1:1로 고정 매핑하여, 실제 내부 네트워크 구조는 외부에 노출하지 않으면서도 필요한 서비스만 외부에 제공합니다.**

**(DMZ 결과)**

**그래서 DMZ에 계층화된 ACL 정책을 적용했습니다.**

**DMZ 구간에서는 외부에서 들어오는 모든 트래픽을 기본적으로 허용하지 않고,**

**오직 본사와 지사, 그리고 DR 센터에서 들어오는 SSH와 ICMP 트래픽만 허용하도록 설정했습니다.**

**이렇게 함으로써 외부에서의 불필요한 접근은 모두 차단하고,**

**지사와 본사, DR 센터에서 필요한 관리 트래픽만 안전하게 허용할 수 있도록 했습니다.**

**또한, OSPF 라우팅 트래픽과 기존에 설정된 연결은 별도로 허용하여 네트워크 운영에 지장이 없도록 하였고,**

**외부에서 들어오는 모든 SSH 트래픽과 그 외의 모든 IP 트래픽은 명확히 차단하여 무차별 대입 공격 등 보안 위협을 원천적으로 차단했습니다.**

**이 정책은 외부 인터페이스에 인바운드 방향으로 적용되어, 본사와 지사 네트워크의 필수 트래픽만 선택적으로 허용하고 외부 공격은 차단하는 구조입니다.**

**이상입니다.**

**다음 발표자 오수연님에게 넘기겠습니다.**

**발표자 5 방민우**

**안녕하세요. 자동화 부분을 맡은 방민우 입니다.**

**ATM 장비 도입 시 발생한 방화벽 보안 정책 누락 문제를 해결하기 위한 자동화 프로젝트를 수행했습니다.**

**신규 ATM 장비가 전국적으로 도입되면서,**

**기존 방화벽 정책 템플릿에 신규 장비에 대한 정책이 누락되어,**

**보안 포트가 외부에 그대로 노출되는 상황이 발생했습니다.**

**이로 인해 외부 장비에서 ATM 보안 port로의 접근이 가능해지는 심각한 보안 위협으로 이어질 수 있었고,**

**이에 따라 신속한 대응과 체계적인 정책 관리 시스템 구축이 필요했습니다.**

**저희는 이를 해결하기 위해**

**Ansible 기반의 자동 배포 Playbook을 설계했습니다.**

**신규 장비가 추가되면,**

**인벤토리에 등록된 방화벽 장비에**

**ACL 정책이 적용되도록 구성했으며,**

**정책 적용 이후 장애가 발생할 가능성도 고려해**

**롤백용 Playbook도 함께 구성하여, 언제든지 정책을 즉시 되돌릴 수 있도록 했습니다.**

**이 시스템을 통해 정책 누락 없이**

**전국 수백 대 ATM 장비의**

**네트워크 접근을 제어하는**

**보안 정책을 방화벽에 일괄 적용할 수 있었고,**

**자동화와 표준화를 통해 운영 효율성과 네트워크 안정성을 동시에 확보할 수 있었습니다.**

**플레이북은 이렇게 작성했습니다.**

**테스트 환경에서는 텔넷 포트를 차단하는 ACL을 자동 적용하고,**

**필요 시 다시 제거하는 시나리오를 구성하여**

**작성해 보았습니다.**

**실제 업무 환경을 고려하여**

**특정 아이피 혹은 Prefix를 차단하는 플레이북도 함께 작성해 보았습니다.**

**지금부터 그 과정을 영상으로 보여드리겠습니다.**

**감사합니다.**