**NAT창선 NETWORKS  
네트워크 설계 보안 기술 가이드**

네트워크 설계 및 사용자 설명서

# 개요

더본코리아의 나마을식당은 대규모 식당 사업을 위해 네트워크 인프라를 새롭게 구축하는 프로젝트입니다. 이 프로젝트는 네트워크 운영의 효율성과 안정성을 극대화하고, 네트워크 보안을 위해 NAT, ACL, VPN기술을 활용합니다. 이 명세서는 해당 프로젝트에서 보안 기술의 구현 및 구성에 대해 설명합니다.

## 요구사항

더본코리아/나마을식당 측에서 제시한 요구사항은 다음과 같습니다.

* <요구 사항 1: 외부와 내부 네트워크를 분리하여 통신하는 구조를 구현합니다.>
* <요구 사항 2: 허용되지 않은 IP 주소에 대한 접근을 제어합니다.>
* <요구 사항 3: : 특정 포트로의 접근을 제어하여 네트워크 보안을 강화합니다.   
  이를 위해, SSH, Telnet 등의 서비스에 대한 접근 제어를 수행합니다.>
* <요구 사항 4: 본사와 지사간의 안전한 통신을 위한 방안을 마련합니다.>

## 솔루션

* 솔루션 1: NAT 및 ACL을 활용하여 사설 IP와 공인 IP를 분리합니다. 이를 통해 내부 네트워크와 외부 네트워크를 분리하고 접근을 제어합니다.
* 솔루션 2: 특정 IP 및 포트에 대한 ACL 정책을 설정하여 허용되지 않은 사용자에 대한 접근을 제어합니다.
* 솔루션 2-1: 네트워크 장비에는 관리자만이 SSH를 통해 접근할 수 있도록 ACL 및 SSH 설정을 수행합니다.
* 솔루션 3: VPN 기술을 활용하여 본사와 지사간의 통신을 암호화합니다.

Core 계층의 종단 장치에 ACL 정책을 설정하여 외부와 내부 트래픽에 대한 접근을 제어합니다. 이와 함께 NAT 기능을 설정하여 외부/내부 네트워크 대역을 분리하고, 외부 접근으로부터 내부 IP를 보호합니다.

**설계**

더본코리아/나마을식당의 인프라 구축에 있어 사용된 HA 기술에 대한 적용 범위 및 방법을 명세합니다.

**기술 소개**

- **ACL(Access Control List)**: 허가되지 않은 이용자가 네트워크 장비나 특정 서버에 접근하려고 하는 것을 차단하는 기술

**기능**

1) 내부적인 패킷 필터링

2) 부적절한 접근으로부터의 내부 네트워크 보호

3) 포트들에 대한 정책 설정으로 특정 서비스의 이용 제한

- **NAT(Netwrok Address Translation):**  IP 패킷의 TCP/UDP 포트 숫자와 소스 및 목적지의 IP 주소 등을 재기록하면서 라우터를 통해 네트워크 트래픽을 주고받는 기술

**기능**

1) 공인 IP주소 절약

2) 외부/내부 네트워크 분리를 통한 내부 네트워크 보호

- **VPN(Virtual Private Network):** 가상 사설 네트워크라고도 하며, 인터넷을 통해 데이터를 안전하고 보안적으로 전송하기 위해 사용되는 기술

**기능**

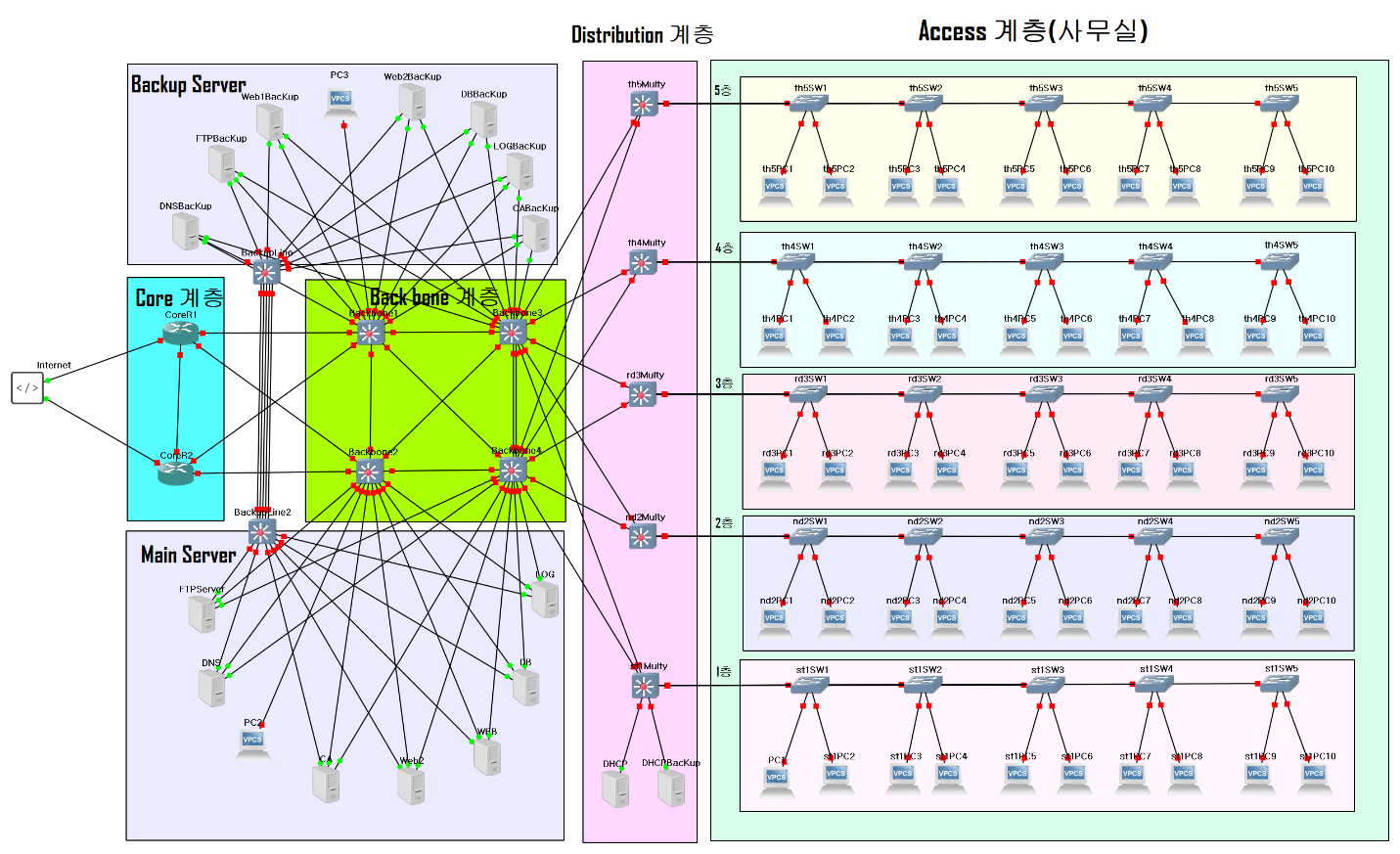
1 )전송하는 데이터를 암호화하여 외부로부터 보호

2) VPN IP를 통해 데이터를 전달함으로써 실제 IP 주소 보호

**적용 범위**

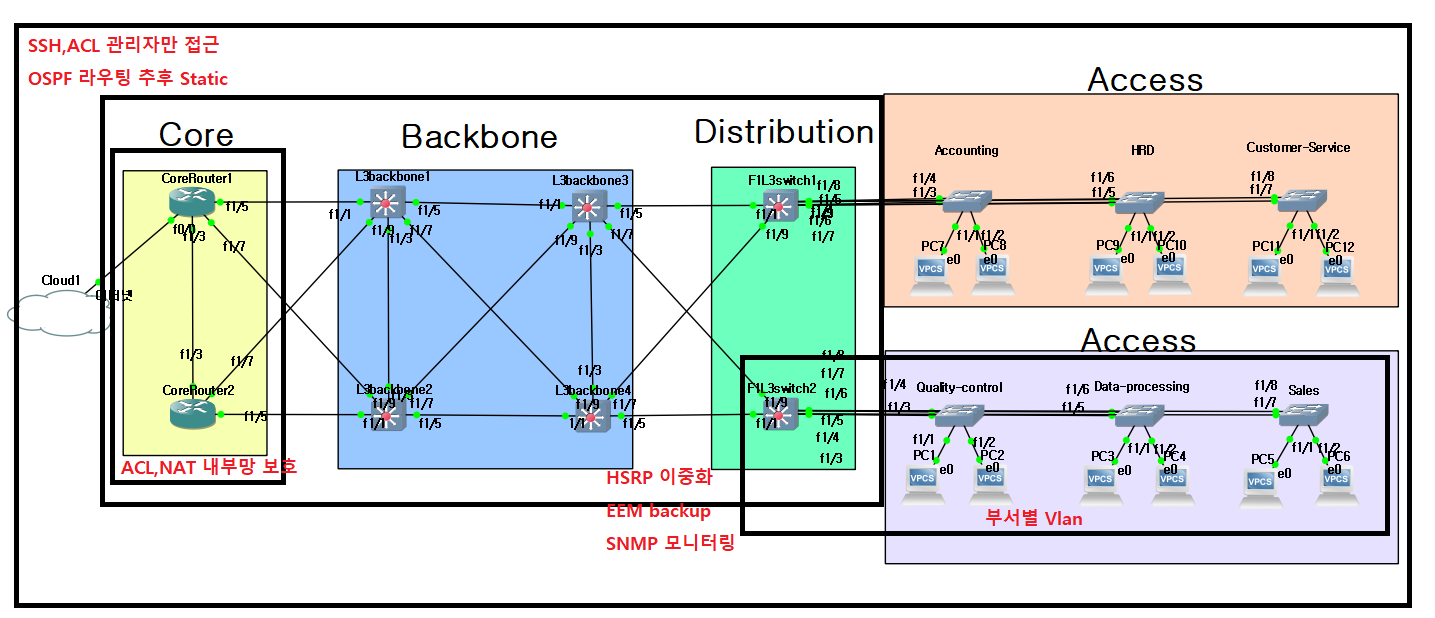
이 프로젝트의 네트워크 보안 기술들은 더본코리아의 나마을식당 본사와 경기지사, 그리고 서울지사에서의 네트워크 인프라 구축에 모두 적용됩니다. 즉, 각 지사와 본사의 네트워크 인프라에 ACL, NAT, 그리고 VPN 기술이 도입되어, 외부로부터의 보안 위협을 최소화하고 안전한 데이터 통신을 지원합니다. 이를 통해 각 지사와 본사는 안정적이고 효율적인 네트워크 시스템을 이용할 수 있게 됩니다. 이렇게 세 식당 모두에서 사용되는 통합된 네트워크 시스템은 일관된 경험을 제공하며, 기업 전체의 네트워크 관리를 간편하게 만듭니다.

- **본사**



* BackBone 계층의 Router 4개
  + 적용 솔루션
    - 솔루션 2-1: SSH에대한 ACL정책
* Core 계층의 Router 2개
  + 적용 솔루션
    - 솔루션 1: NAT
    - 솔루션 2-1: SSH에대한 ACL정책, 웹 서비스 포트에 대한 ACL 정책
    - 솔루션 3 : VPN
* Disrtibution 계층의 Router 5 개
  + 적용 솔루션
    - 솔루션 2-1: SSH에대한 ACL정책

- 지사



* BackBone 계층의 Router 4개
  + 적용 솔루션
    - 솔루션 2-1: SSH에대한 ACL정책
* Core 계층의 Router 2개
  + 적용 솔루션
    - 솔루션 1: NAT
    - 솔루션 2-1: SSH에대한 ACL정책, 웹 서비스 포트에 대한 ACL 정책
    - 솔루션 3 : VPN
* Disrtibution 계층의 Router 2 개
  + 적용 솔루션
    - 솔루션 2-1: SSH에대한 ACL정책

## 기술 설계

각 솔루션에 해당하는 실제 설계에 명세합니다.

**솔루션 1) NAT,ACL 설정 가이드**

* **본사 Core**

|  |
| --- |
| conf t  access-list 130 permit ip any any  ip nat inside source list 130 interface GigabitEthernet0/0 overload  int gi0/0  ip nat outside  int range gi1/0  ip nat inside  int range gi2/0  ip nat inside  int range gi3/0  ip nat inside |

* **지사 Core**

|  |
| --- |
| conf t  access-list 101 permit ip any any  ip nat inside source list 101 interface fa0/0 overload  int fa0/0  ip nat outside  int fa1/3  ip nat inside  int fa1/5  ip nat inside  int fa 1/7  ip nat inside |

**솔루션 2) ACL 설정 가이드**

* 네트워크 장비에 관리자만 SSH를 통해 접근 가능하도록 ACL 및 ssh 설정

|  |
| --- |
| access-list 10 permit 172.20.1.10 0.0.0.0  access-list 10 permit 172.20.2.10 0.0.0.0  access-list 10 deny any  line vty 0 4  access-class 10 in |

**솔루션 3) VPN(IPSec Site to Site) 설정 가이드**

* 본사

|  |
| --- |
| crypto isakmp policy 10  encryption 3des  hash md5  authentication pre-share  lifetime 2600  group 2  crypto isakmp key gyeonggido address 192.168.1.250    access-list 100 permit ip 172.20.0.0 0.0.255.255 172.22.0.0 0.0.255.255  crypto ipsec transform-set gyeonggido esp-3des esp-sha-hmac  crypto map IPSEC 10 ipsec-isakmp  set peer 192.168.1.250    set transform-set gyeonggido  match address 100  int fa0/0  crypto map IPSEC |

* crypto isakmp key gyeonggido address 공인IP주소(공유기 DHCP 할당 IP주소)
* set peer 공인IP주소(공유기 DHCP 할당 IP주소)
* **지사**

|  |
| --- |
| crypto isakmp policy 10  encryption 3des  hash md5  authentication pre-share  lifetime 2600  group 2  crypto isakmp key hq address 192.168.1.224    access-list 100 permit ip 172.22.0.0 0.0.255.255 172.20.0.0 0.0.255.255  crypto ipsec transform-set hq esp-3des esp-sha-hmac  crypto map IPSEC 10 ipsec-isakmp  set peer 192.168.1.224    set transform-set hq  match address 100  int fa0/0  crypto map IPSEC |

* crypto isakmp key hq address (본사의 공인 IP주소(공유기 DHCP 할당 IP주소)
* set peer (본사의 공인 IP주소(공유기 DHCP 할당 IP주소)

**설계 확인**

**솔루션 1**

* NAT 및 ACL을 활용하여 사설 IP와 공인 IP를 분리합니다. 이를 통해 내부 네트워크와 외부 네트워크를 분리하고 접근을 제어합니다.

|  |  |
| --- | --- |
| **설계 확인** | |
|  | |
| **설명** | 본 설계에서는 Core Router를 통해 NAT(Network Address Translation)를 구현하였습니다. 이를 위해 Core Router에 적절한 access-list를 지정한 후, 'ip nat inside source' 명령어를 사용하여 해당 조건에 맞는 IP들이 변환되어 외부로 나가게 되는 과정을 설정하였습니다.  현재 설정 상태에서는 모든 IP가 gigabitEthernet 0/0의 IP로 변환되어 외부와 통신하도록 설정되어 있습니다. 이렇게 NAT 기능을 활용하여 사설 IP를 공인 IP로 변환하면 외부와의 정상적인 통신이 가능해집니다.  NAT를 활용하면 내부 네트워크와 외부 네트워크를 분리함으로써 네트워크의 안정성을 향상시킬 수 있습니다. 하지만 주의해야 할 점은 NAT 프로토콜만을 사용할 경우, 외부에서 내부 네트워크로의 접근이 불가능하게 되므로 이 점을 고려한 접근 제어 정책을 설정해야 합니다. 이렇게 NAT 기능을 적용함으로써 더본코리아/나마을식당의 네트워크는 외부로부터의 보호를 강화하고, 동시에 효율적인 IP 주소 관리를 실현할 수 있게 되었습니다. |

**솔루션 2**

* 본 설계에서는 Access-list(ACL)를 활용하여 특정 IP에 대한 접근을 제어하였습니다. 이를 통해, 특정 IP의 접근을 차단하거나 허용하는데 필요한 정책을 구현할 수 있습니다.

|  |  |
| --- | --- |
| **설계 확인** | |
|  | |
| **설명** | 본 사업에서는 관리용 PC가 존재하는 172.20.1.0/24, 172.20.2.0/24 네트워크 대역만 SSH 접속을 허용하는 ACL을 설정하였습니다. 이 밖에도 인터페이스, NAT 등 다양한 분야에서 ACL을 사용하였습니다.  ACL의 구성은 Standard와 Extended 모드로 나뉩니다.   * Standard 모드는 099, 13001999 번 대에서 사용 가능하며, 이는 출발지의 IP만 필터링 가능합니다. * Extended 모드는 100199, 20002699번 대에서 사용 가능하며, 출발지와 목적지, 프로토콜, 포트별로 필터링이 가능합니다. |
|  | |
| **설명** | 설정 결과, 관리용 네트워크 대역이 아닌 CoreR1에서 Backbone3로 SSH 접속 시에 접근이 차단된 것을 확인하였습니다. |
|  | |
| **설명** | 서버에서 라우터나 스위치에 접근할 때 'key exchange algorithm' 오류가 발생하는 경우가 있을 수 있습니다. 이 경우, 'ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc' 명령어를 사용하여 키 교환 방식을 맞춰주면 정상적으로 접근이 가능합니다.  따라서, 이러한 ACL 설정을 통해 더본코리아/나마을식당의 네트워크는 특정 IP와 포트에 대한 접근을 효과적으로 제어할 수 있게 되었습니다. |

**솔루션 3**

* VPN(Virtual Private Network) 기술을 활용하여 본사와 지사간의 통신을 암호화하였습니다. 이를 통해, 본사와 지사간의 네트워크 트래픽을 안전하게 보호하며, 신뢰성 있는 원격 접속 환경을 제공합니다.

|  |  |
| --- | --- |
| **설계 확인** | |
|  | |
| **설명** | IPsec 명령어를 입력하면 두 기기간의VPN 터널을 만들기 위해 키 교환과 보안 매개변수 협상을 진행하게됩니다. 해당 과정을 통해 사용자 신원 보호와 중간자 공격(Man In The Middle Attack) 을 방지할 수 있습니다. |
|  | |
| **설명** | 해당 협상과정이 종료되고 장비에서 현재 활성화된 ISKMP(VPN)연결상태를 show crypto isakmp sa 명령어를 통해 확인할 수 있습니다. 상대방 및 자신의 터널링에 사용할 IP 주소, 보안 연결 상태(현재 과정에선 Quick Mode를 통한 터널링을 지원합니다.), 보안 연결 식별자, 현재 상태 등을 확인할 수 있습니다. |
|  | |
| **설명** | 현재 IPsec을 통한 데이터 전송 시 ESP 암호화 프로토콜을 통해 인터넷 구간을 지나갈 때 외부에서 패킷을 엿볼 수 없도록 암호화가 진행되어 기밀성을 높일 수 있습니다. 또한 ESP 데이터는 무결성을 보호하기 위해 해시 기반의 인증을 사용함으로 변조 및 간자 공격을 방지하고 확인할 수 있습니다. |