2018 전국기능경기대회 과제

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **직 종 명** | IT Network System | **과제명** | Cisco Environment | **과제번호** | 제 3 과제 |
| **경기시간** | 4시간 | **비번호** |  | **심사위원**  **확 인** | (인) |

1. 과제 개요

당신은 네트워크 아웃소싱 업체의 네트워크 엔지니어 입니다. ADVshow라는 신생 광고회사가 당신에게 네트워크 구성 및 서버 구성 관련 업무를 요청했습니다. 해당 업체는 www.advshow.com 도메인을 통해 외부에서 홈페이지를 접근하기를 원하며 내/외부간 전화를 통한 업무를 할 수 있기를 원합니다. 또한, 해당 네트워크 구축 후 모니터링 및 관리를 외부에서 할 수 있도록 구성되기를 원합니다. 이를 위해서 Cisco 장비를 이용한 VoIP 인프라를 구축하고 리눅스 서버를 이용한 Web Server 및 Monitoring Server를 구축하며, 외부에서 내부로 쉽게 접근할 수 있도록 VPN 서비스를 구축하도록 합니다. 또한, 모든 장비 및 서버는 SSH를 이용하여 관리를 쉽게 할 수 있도록 구성합니다.

1. 배포자료(USB에 복사하여 배포)

• Windows Server 2016 R2 ISO 이미지

• Windows 10 Enterprise(RS) x64 ISO 이미지

• Debian Linux 9.21 Blue-ray 이미지

• VMware Workstation 14

• cipc-admin-fmr.8-6-4-0

• putty.exe

1. 주의 사항

• 암호를 필요로 하는 곳에 암호가 지정되지 않을 경우 “adv2018##”을 기본 값으로 사용합니다.

• 특별하게 지정되지 않은 옵션 또는 설정은 시스템이 추천하는 기본 값을 사용합니다.

• 모든 Guest OS의 프린터 포트, 사운드 장치 및 플로피드라이브를 제거합니다.

• 정해진 USB장치 이외의 저장장치의 반입을 금지합니다.

• 휴대폰 등과 같은 스마트기기는 경기시작 전 심사위원(또는 관리위원)에게 보관합니다.

1. 과제 내용
   1. 기본 구성

부록의 운영체제 설치 항목을 참고하여 운영체제를 설치하도록 합니다.

각 Cisco 장비에 아래와 같이 기본 구성을 하도록 합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 내용 | | 비고 |
| Local User | ID | itnsa | Privilege 15 |
| Password | adv2018## |
| Enable Password | adv2018## (Reversible cipher text, ASA 제외) | |  |

* 1. 네트워크 구성
     1. Routing

EIGRPv6 (AS 1)를 이용하여 IPv6 네트워크의 통신의 문제가 없도록 구성합니다.

IPv4 네트워크의 원할 한 통신을 위해 ADV-R와 ADV-FW 간의 OSPF(area 0)를 사용하도록 합니다.

ADV-R에 Null Routing을 구성하도록 하며, ADV-FW는 OSPF를 통해 모든 트래픽을 ADV-R로 보내도록 합니다.

* + 1. Switching

아래 표를 참고하여 각 스위치에 VLAN을 구성합니다.

|  |  |  |
| --- | --- | --- |
| 구분 | ADV-SW1 | ADV-SW2 |
| VLAN 10 (Server) | fa0/1-fa0/6 |  |
| VLAN 20 (Client) |  | fa0/1-6 |
| VLAN 99 (Management) | fa0/9-12 | fa0/9-12 |
| VLAN 100 (Monitor) |  | |

통신에 문제가 없도록 적절히 Trunk 설정을 하도록 합니다.

EtherChannel

ADV-SW1과 ADV-SW2의 fa0/13-fa0/14 포트에 표준 프로토콜을 이용하여 Etherchannel을 구성합니다.

ADV-SW1은 EtherChannel 패킷을 송신하여 다른 포트와 협상을 할 수 있도록 합니다. ADV-SW2은 EtherChannel 패킷의 전송을 최소화 하도록 구성합니다.

각 스위치에 구성된 Etherchannel은 VLAN 100 Traffic만 지나가도록 구성합니다.

Client VLAN

Client VLAN에 연결된 Port는 STP 계산 없이 Forward 상태가 되도록 합니다.

보안을 위해 "Client VLAN" Port는 Superior BPDU 수신 시 root-inconsistent 상태가 되도록 합니다.

Flexible Authentication

"Client VLAN"에 연결된 Port에 Port Authentication 설정을 하도록 합니다.  
VoIP 장비들은 Mac Address 인증을 통해 연결될 수 있도록 하며, PC들은 사용자 인증을 통해 연결될 수 있도록 합니다. PC연결에 따른 사용자 인증을 우선으로 합니다.

DHCP Snooping

ADV-SW2에 Vlan20에 대한 DHCP Snooping을 구성하도록 합니다. Switch에서 DHCP 요청 패킷에 Option 82 값을 추가하도록 합니다.

클라이언트가 Fa0/3 포트에 연결되면 192.168.0.201, Fa0/4 포트에 연결되면 192.168.0.202 주소를 할당받도록 구성합니다.

Switch Port Analyzer

ADV-SW1에서 VLAN10을 지나는 모든 트래픽을 Monitor Vlan 으로 보내도록 합니다. ADV-SW2는 Monitor Vlan 으로부터 오는 모든 트래픽을 Mon-PC가 연결되어 있는 Port로 보내도록 합니다.

Dynamic VLAN

ADV-SW2의 Fa0/5 포트에서 Dot1x 인증 시 guest 사용자를 사용하면 VLAN 1이 Access VLAN으로 설정되고, vlan 사용자를 사용하면 VLAN 20이 Access VLAN으로 설정되도록 합니다.

Gateway 구성

ADV-SW1 및 ADV-SW2는 동적으로 기본 게이트웨이를 찾도록 합니다.

ADV-SW1은 192.168.0.126, ADV-SW2는 192.168.0.254가 게이트웨이입니다.

* 1. 서버 구성
     1. DNS 서비스

ADV-SRV에 advshow.com 도메인의 Bind9을 아래의 조건에 따라 구성합니다.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location | Host | Domain | Type | Value |
| Internal | ADV-R | advshow.com | A | 192.168.0.126 |
| ADV-FW | A | 192.168.0.125 |
| ADV-SRV | A | 192.168.0.1 |
| www | CNAME | ADV-SRV.advshow.com |
| mon | CNAME | ADV-SRV.advshow.com |
| External | www | advshow.com | AAAA | 2001:db8:4::2 |
| manager | AAAA | 2001:db8:4::3 |
| vpn | AAAA |

DHCP 서비스

ADV-SRV에 Client Network를 위한 DHCP Service를 구성하도록 합니다. 아래 표를 참고하여 구성하며, 추가 옵션이 필요할 경우 적절히 추가하도록 합니다.

|  |  |
| --- | --- |
| 구분 | 내용 |
| Network | 192.168.0.128/25 |
| Range | 192.168.0.150 ~192.168.0.200 |
| DNS Server | 192.168.0.1 |
| Domain | advshow.com |

EX-R에 2001:db8:2::/64 Network를 위한 DHCPv6 Service를 구성하도록 합니다. 아래 표를 참고하여 구성하도록 합니다.

|  |  |
| --- | --- |
| 구분 | 내용 |
| Network | 2001:db8:2::/64 |
| DNS Server | 2001:db8:4::2 |
| M flag | enable |
| O flag | enable |

RADIUS 서비스

인증을 위한 Radius 서버를 ADV-SRV에 구성합니다. 내부 네트워크 장비들의 인증을 위한 계정을 아래 표를 참고하여 구성합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| Account | password | Privileged mode | 비고 |
| admin | admin2018## | 15 | Management |
| user | user2018## | 1 |
| vpn | vpn2018## | 1 | VPN authentication |
| dot1x | dot1x2018## | 1 | Dot1x authentication |
| guest | vlan2018## | 1 |
| vlan | vlan2018## | 1 |

장비 콘솔 접속 시, Radius 인증을 하도록 합니다. 또한 Radius 서버와 연결이 끊겼을 경우, 로컬 데이터베이스 계정을 통해 장비에 접속할 수 있도록 합니다.

* 1. 서비스 구축
     1. Remote Management

ADV-R, ADV-FW, ADV-SW1, ADV-SW2에 TELNET 원격 접속을 구성합니다.

ADV-SRV에서 제공하는 Radius 인증을 통해 VTY line에 연결되도록 합니다.

내부 네트워크 Management VLAN를 통해서만 원격 접속이 가능해야 합니다.

Logging

ADV-R, ADV-FW, ADV-SW1, ADV-SW2의 Log를 ADV-SRV에 Logging 합니다.

모든 로그는 Informational 정보를 포함해야 하며, Log 파일은 아래 형식을 참고합니다.

|  |  |
| --- | --- |
| 구분 | 형식 |
| 전체 로그 | /var/log/cisco/all.log |
| 장비별 로그 | /var/log/cisco/**hostname**.log |

Web Log Management

제공된 파일을 이용하여 ADV-SRV에 Loganalyzer 서버를 구성하도록 합니다. /var/log/cisco/all.log 파일을 Source 파일로 사용하도록 합니다.  
"http://mon.advshow.com"을 통해 접속하도록 합니다.

SNMP 모니터링

ADV-R, ADV-FW, ADV-SW1, ADV-SW2 장비에 아래 표를 참고하여 SNMP 구성을 하도록 합니다. 또한, ADV-SRV에서 snmp package를 설치하여 SNMP 값을 불러올 수 있도록 합니다.

|  |  |
| --- | --- |
| 구분 | 내용 |
| Type | Read-only |
| community | snmp\_ro |
| location | JeonNam, Korea |
| contact | admin@advshow.com |

Cacti 모니터링

ADV-SRV의 Cacti package를 이용하여 ADV-R, ADV-FW, ADV-SW1, ADV-SW2 의 Interface를 모니터링 하도록 합니다.

"http://mon.advshow.com/cacti"을 통해 접속하도록 합니다.  
접속 시 "ID : admin, Password : adv2018##"으로 인증되도록 구성합니다.

Backup

ADV-R, ADV-SW1, ADV-SW2 running-configuration을 저장 시 ADV-SRV의 /ftp/backup/<hostname>-<time>.cfg 파일에 Backup 되도록 합니다. Backup 시 ADV-SRV의 FTP 서비스를 사용하도록 합니다.

Network Time Synchronize

EX-R에 stratum 1 NTP Server를 구성합니다. ADV-R은 EX-R을 통해 NTP 정보를 받아오며 내부를 위한 NTP Server로 동작합니다. EX-R과 ADV-R 간의 NTP 정보 업데이트를 위해 md5 인증을 사용합니다.

모든 장비의 Time-zone을 KST (GST +9)로 설정합니다.

Certificate Authority

ADV-R에 아래 조건에 따라 인증기관을 설치하며 SSL/TLS통신을 위한 인증서를 제공할 수 있도록 합니다.

|  |  |
| --- | --- |
| 인증기관 이름 | ADV\_Show\_CA |
| 인증기관 유형 | Standalone CA |
| Database 경로 | ADV-SRV의 /ftp/ca (FTP 이용) |

Web Service

ADV-SRV에 내부 사용자를 위한 HTTP 서비스를 구성합니다. 해당 사이트 접속 시 “This is Internal Web Site” 라는 문구가 표시되어야 합니다.

해당 사이트 접속 시 "ID : **admin**, Password : **admin2018##**"으로 인증되도록 구성합니다.

ADV-SRV에 외부 사용자를 위한 HTTPS 서비스를 구성합니다. 해당 사이트 접속 시 "This is External Web Site. So you need to use HTTPS for security" 라는 문구가 표시되어야 합니다.

FTP Service

File 이동의 편의를 위하여 ADV-SRV에 FTP 서버를 구성합니다. FTP 접속 시 "ID : **ftpuser**, Password : **ftp2018##**"를 로그인 정보로 이용하여 접속 하도록 하며, /ftp를 기본 디렉토리로 사용합니다.

Network Securing 모니터링

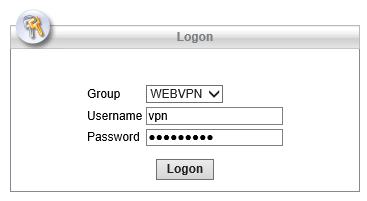
"Switch Port Analyzer"를 통해 들어오는 패킷을 확인할 수 있도록 Mon-PC에   
오픈소스 IDS/IPS 소프트웨어인 Suricata를 설치하고 ICMP 메시지가 발견될 경우 /var/log/suricata/fast.log 파일에 로그를 남깁니다. 요구되지 않은 사항은 기본 설정을 그대로 사용합니다.

**alert icmp any any -> any any (msg:"ICMP detected";)**

* 1. **VPN 구성**
     1. WebVPN

외부에서 내부 자원 접근 및 장비 관리를 위해 ADV-FW에 Clientless VPN을 구성합니다. VPN 연결을 위해 ADV-SRV를 통한 RADIUS 사용자 인증을 구성합니다.

외부 호스트에서 "https://vpn.advshow.com" 접속 시 아래와 같은 인증을 통해 VPN에 연결할 수 있도록 합니다.



* + 1. 추가 기능 구현

"admin" 계정 로그인을 통해 Clientless VPN 접속 시 "http://www.advshow.com"에 인증없이 들어갈 수 있도록 구성합니다.

외부에서 TELNET을 통하여 ADV-R, ADV-SW1, ADV-SW2에 접속할 수 있도록, ADV-FW에 플러그인을 구성하도록 합니다.

* + 1. AnyConnect VPN

WebVPN으로 불가능한 자원 접근 및 관리가 필요한 상황을 위해 ADV-FW에 AnyConnect VPN을 구성합니다. VPN 연결을 위해 ADV-SRV에서 RADIUS 사용자 인증을 구성합니다.

Manager 클라이언트에 AnyConnect Secure Mobility Client를 설치합니다.

접속 시 192.168.1.0/24 대역의 IP 주소를 받아옵니다.

접속 후 내부 네트워크에 접근할 수 있어야 합니다.

* 1. **VoIP 구성**
     1. Domain 내부의 통화가 가능하도록 다음 표를 참고하여 VoIP를 구성합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| HOST | User | Number | CME Server |
| ADV-Phone01 | Alice | 1001/1002 | ADV-R |
| ADV-Phone02 | Bob | 1003/1004 | ADV-R |

모든 IP Phone에 사용자 이름이 보여져야 하며, 전화 연결 시 번호 대신 사용자 이름이 출력될 수 있도록 설정합니다.

IP Phone에 "advshow.com"이라는 도메인 명을 부여합니다.

IP Phone의 배경 이미지를 “worldskills.png”로 변경합니다.

IP Phone의 벨소리를 “hello.raw”로 변경합니다.

1001번 및 1002번으로 전화가 올 시 기능 벨소리가 울리도록 구성합니다.

* 1. **Security 구성**
     1. NAT-PT

아래 표를 참고하여 통신을 위한 NAT-PT를 ADV-R에 구성하도록 합니다.

|  |  |  |
| --- | --- | --- |
| 구분 | IPv4 | IPv6 |
| 정적 NAT-PT | 192.168.0.1 | 2001:db8:4::2 |
| 192.168.0.125 | 2001:db8:4::3 |
| 동적 NAT-PT | 10.20.30.0/24 | 외부 IPv6 Networks |

HTTP Block

ADV-R에서 설정합니다. 전송되는 HTTP 패킷 중 URL에 아래 단어가 포함되는 접속 시도가 발견되면 ADV-R 라우터에서 접속을 차단합니다.

**advblock, blockplus, blockads**

ASA Firewall

토폴로지를 참조하여, ASA-FW의 방화벽 설정을 구성합니다.  
필요한 통신을 위해서만 ACL를 사용하도록 합니다.  
(ASA를 통과하는 모든 트래픽이 허용되지 않도록 합니다.)

1. Logical Topology ( Overview )



1. Logical Topology ( Management & Monitoring )



1. Interface Mapping Table

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADV-SW1 | | | | | | | | |
| Device | Interface | fa0/1 | fa0/6 | fa0/7 | fa0/9 | fa0/10 | fa0/13 | fa0/14 |
| ADV-SRV | NIC |  |  |  |  |  |  |  |
| ADV-FW | eth1 |  |  |  |  |  |  |  |
| eth7 |  |  |  |  |  |  |  |
| ADV-R | fa0/0 |  |  |  |  |  |  |  |
| ADV-SW2 | fa0/9 |  |  |  |  |  |  |  |
| fa0/13 |  |  |  |  |  |  |  |
| fa0/14 |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADV-SW2 | | | | | | | | |
| Device | Interface | fa0/1 | fa0/2 | fa0/6 | fa0/9 | fa0/13 | fa0/14 | fa0/15 |
| ADV-Phone01 | SW |  |  |  |  |  |  |  |
| ADV-Phone02 | SW |  |  |  |  |  |  |  |
| Mon-PC | NIC0 |  |  |  |  |  |  |  |
| ADV-FW | eth0 |  |  |  |  |  |  |  |
| ADV-SW1 | fa0/10 |  |  |  |  |  |  |  |
| fa0/13 |  |  |  |  |  |  |  |
| fa0/14 |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| EX-R | | | |
| Device | Interface | fa0/0 | fa0/1 |
| ADV-R | fa0/1 |  |  |
| Manager | NIC0 |  |  |

1. IP address Table

|  |  |  |
| --- | --- | --- |
| Vlan 10 (Server) | | |
| Host | Interface | IP address |
| ADV-R | Fa0/0.10 | 192.168.0.126/25 |
| ADV-FW | DMZ | 192.168.0.125/25 |
| ADV-SW1 | Vlan10 | 192.168.0.124/25 |
| ADV-SRV | ens?? | 192.168.0.1/25 |

|  |  |  |
| --- | --- | --- |
| Vlan 20 (Client) | | |
| Host | Interface | IP address |
| ADV-FW | Client | 192.168.0.254/25 |
| ADV-SW2 | Vlan20 | 192.168.0.253/25 |
| ADV-Phone01 | Switch | DHCP |
| ADV-Phone02 | Switch | DHCP |
| CLI-PC | NIC0 | DHCP |
| Mon-PC | NIC0 | none |

|  |  |  |
| --- | --- | --- |
| Vlan 99 ( Management) | | |
| Host | Interface | IP address |
| ADV-SW1 | Vlan99 | 1.1.1.1/24 |
| ADV-SW2 | vlan99 | 1.1.1.2/24 |
| ADV-R | fa0/0.99 | 1.1.1.3/24 |
| ADV-FW | Management | 1.1.1.4/24 |

|  |  |  |
| --- | --- | --- |
| 2001:DB8:1::/64 | | |
| Host | Interface | IP address |
| ADV-R | fa0/1 | 2001:DB8:1::1/64 |
| EX-R | fa0/0 | 2001:DB8:1::2/64 |

|  |  |  |
| --- | --- | --- |
| 2001:DB8:2::/64 | | |
| Host | Interface | IP address |
| EX-R | fa0/1 | 2001:DB8:2::1/64 |
| Manager | NIC0 | DHCPv6 |

|  |  |  |
| --- | --- | --- |
| Loop Back | | |
| Host | Interface | IP address |
| ADV-R | loopback 100 | 2001:DB8:3::1/64 |
| loopback 200 | 2001:DB8:4::1/64 |

1. **운영체제 설치**
   1. ADV-SRV

|  |  |
| --- | --- |
| 컴퓨터이름 | ADV-SRV |
| 운영체제 | Debian Linux 9.21 x64 |
| 도메인이름 | Advshow.com |
| 암호 | adv2018## |

* 1. CLI-PC

|  |  |
| --- | --- |
| 컴퓨터이름 | CLI-PC |
| 운영체제 | Window 10 Enterprise x64 |
| 도메인이름 | Advshow.com |
| 추가사용자 | advertiser |
| 암호 | adv2018## |

* 1. Mon-PC

|  |  |
| --- | --- |
| 컴퓨터이름 | Mon-PC |
| 운영체제 | Debian Linux 9.21 x64 |
| 도메인이름 | Advshow.com |
| 추가사용자 | monitor |
| 암호 | adv2018## |

* 1. Manager

|  |  |
| --- | --- |
| 컴퓨터이름 | Manager |
| 운영체제 | Window 10 Enterprise x64 |
| 추가사용자 | manager |
| 암호 | adv2018## |