시스템 보안 강화 가이드

V3.0 (2016.5)

kt

본 가이드는 ucloud biz 에서 시스템 구축 시 보안 강화를 위한 지침을 담고 있습니다. 보안 침해 사고(해킹 등)의 경우 사용자의 관리 영역이기 때문에, 실제 발생했을 경우 책임 소재가 사용자에 있고 kt 에서 지원 및 책임이 어렵기 때문에 아래 내용을 잘 숙지하여 안전한 시스템을 구축하시기 바랍니다.

1. 가상라우터의 설정

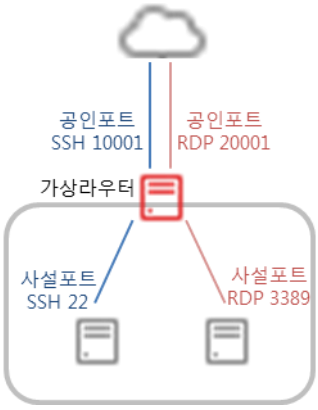
가상라우터는 각 계정의 앞단에서 포트포워딩을 통하여 공인망과 VM 의 사설망을 연결해주는 역할을 합니다. 가상라우터의 설정을 통하여 보안을 강화할 수 있습니다.

A. 포트포워딩을 통한 보안 강화

i. 공인망에서는 알려진 포트(well-Known port)를 통한 침입 시도가 많습니다. (port scanning)

ii. 그렇기 때문에 공인포트를 well-known port 그대로 open 하면 보안적으로 취약해집니다.

iii. 공인포트를 실제 연결하는 사설포트와 다른 번호(unknown port)로 포트포워딩하여 이 취약점을 보완할 수 있습니다.



<그림 1. 포트포워딩 예시>

B. 가상라우터 방화벽 기능을 통한 보안 강화

i. 가상라우터의 방화벽 기능을 통하여 ACL inbound 제어가 가능합니다.

ii. 포탈 콘솔 > ucloud server > 네트워크 > 대상 공인 IP 선택 후 하단 방화벽에서 inbound 허용 정책을 설정할 수 있습니다. 포트포워딩이 추가된 포트에 대해

자동으로 ANY OPEN 됩니다. (0.0.0.0/0) SSH 등과 같이 critical 한 포트는(SSH, DB 등) 실제로 접속할 사용자의 IP(대역)로 제한하여 사용 하시기를 권고 드립니다.)

Source CIDR	Protocol	Start Port	End Port	삭제 및 수정
0.0.0.0/0	tcp	80	80	수정 | 삭제
172.20.10.0/24	tcp	20001	20001	수정 | 삭제
172.20.10.0/24	tcp	10001	10001	수정 | 삭제

<그림 2. 방화벽 설정 화면 예>

2. VM 의 설정

사용자가 VM 내부에서 설정할 수 있는 보안 강화 방법에 대하여 여러 레퍼런스를 제공하고 있습니다.

A. SSH key 를 통한 로그인 설정 (Linux)

i. ucloud server 는 기본적으로 ID/Password 방식의 로그인 방식을 제공합니다. ID/password 방식은 패스워드 해킹에 취약하기 때문에 SSH key 방식의 로그인 설정으로 보안성을 높일 수 있습니다.

ii. SSH Key 를 생성/적용하는 방법은 아래 링크를 참고하시기 바랍니다.

iii. http://cafe.naver.com/ucloudbiz/169 http://cafe.naver.com/ucloudbiz/170

B. VM 패스워드 변경 정책 설정

i. 패스워드의 탈취를 방지하기 위하여 OS 에서 패스워드 글자수와 변경 주기를 강제할 수 있습니다.

ii. 패스워드 변경 정책 설정에 대한 자세한 방법은 아래 링크를 참고하시기 바랍니다.

iii. https://ucloudbiz.olleh.com/manual/Security_Password_change.pdf

C. Fail2Ban 적용 (Linux)

i. 패스워드 해킹은 SSH/FTP 등으로 접속 시도하여 무작위 패스워드를 수없이 반복 입력하여 침입합니다. Fail2Ban 은 무작위로 로그인하는 brute force attack 에 대응하는 모듈입니다.

ii. Fail2Ban 설치 및 설정에 대한 자세한 방법은 아래 링크를 참고하시기 바랍니다.

iii. https://ucloudbiz.olleh.com/manual/Security_fail2ban.pdf

D. root login 제한 (Linux)

i. 다른 user 와 다르게 root user 가 탈취 당했을 때는 위험도가 더 큽니다. 또한 무한 스캐닝 방법의 접속 시도 역시 root 를 통해서 시도됩니다. root user 의 접속을 막는 것이 서버 보안에 많은 도움이 됩니다.

ii. sshd config 에서 root login 제한을 막는 자세한 방법은 아래 링크를 참고하시기 바랍니다.

iii. https://ucloudbiz.olleh.com/manual/Security_sshd_config_root_login_Limited.pdf

E. VM 의 OTP 방식 로그인 설정

i. 은행거래나 ucloud biz 포탈 로그인처럼 OTP(One-Time Password)를 VM 로그인에 적용할 수 있습니다. 한 예로 Google Authenticator 를 이용한 OTP 로그인을 VM 에 설정할 수 있습니다..

ii. Google Authenticator 를 VM 에 적용하는 자세한 방법은 아래 링크를 참고하시기 바랍니다.

iii. http://cafe.naver.com/ucloudbiz/129

F. OS 의 방화벽 활성화

i. OS 에서 방화벽 활성화를 통하여 접속 가능한 대상(서비스)를 선별할 수 있습니다. Linux 의 iptables, Windows 의 방화벽을 사용할 수 있습니다.

G. 보안 솔루션 혹은 보안 서비스 사용

i. 서버 내 백신, 웹 쉘 방어, DB 보안 등의 솔루션을 사용하여 VM 을 보호할 수 있습니다.

H. 보안성 검사 수행

i. KISA 인터넷침해대응센터(http://www.krcert.or.kr)에서는 각종 보안성 관련 가이드를 제공하고 있습니다. 해당 사이트에서 가이드를 활용하여 보안성 점검 및 가이드를 받을 수 있습니다.

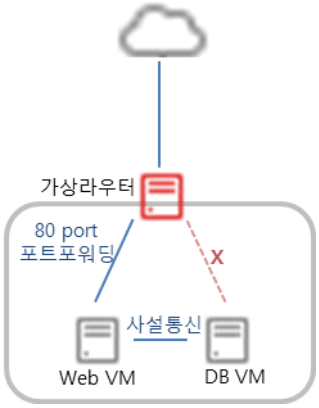
3. 시스템 아키텍처의 보안 강화

시스템 구성(아키텍처)을 통하여 보안성을 강화할 수 있습니다.

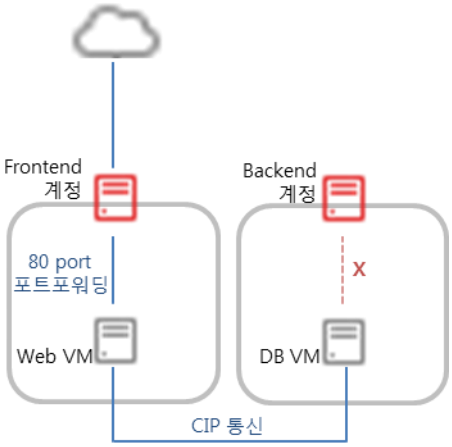
A. Backend 시스템 VM 의 외부 노출 방지

i. 시스템의 backend 시스템 VM(ex. DB)의 경우 포트포워딩을 통한 외부 노출을 지양합니다.

ii. Backend 시스템은 frontend VM 과 사설 IP(혹은 멀티계정 CIP)를 통한 통신만 가능하도록 구성함으로써 주요 backend 시스템을 보호할 수 있습니다.



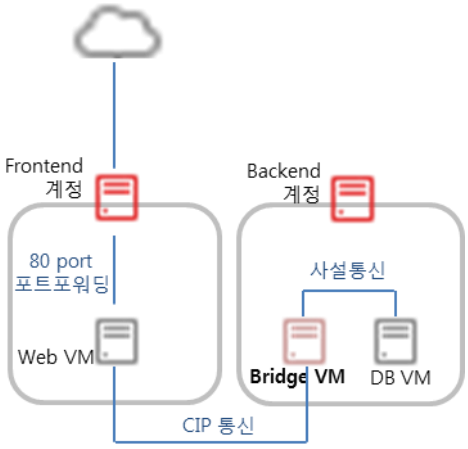
<그림 3. DB VM 의 사설 통신 예>



<그림 4. DB VM 의 별도 계정을 통한 CIP 통신 예>

B. Bridge VM 생성을 통한 계정 분리

i. 멀티계정을 통한 CIP 연동 시 Bridge VM(Linux OS) front-end 계정과 back-end 계정 사이의 방화벽 역할을 하도록 구성할 수 있으며(iptables 기능), 비 인가 패킷에 대해 Drop 처리 및 로깅도 가능합니다. (http://cafe.naver.com/ucloudbiz/70)



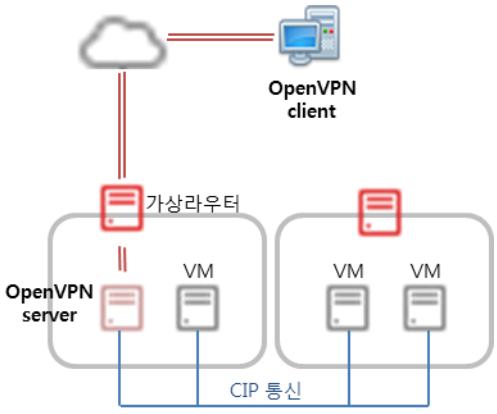
<그림 5. Bridge VM 을 통한 방화벽 사용 예>

ii. Bridge VM 의 구성에 대한 자세한 사항은 아래 링크를 참고하시기 바랍니다.

iii. http://cafe.naver.com/ucloudbiz/70

C. 관리용 OpenVPN 사용

i. 별도 OpenVPN VM 을 두어서 외부에서 직접 서버로 접근이 불가하며, 접근 루트를 일원화 합니다.



<그림 6. OpenVPN 을 통한 외부 접근 제어의 예>

ii. OpenVPN 의 구성 방법은 아래 링크를 참고하시기 바랍니다.

iii. http://cafe.naver.com/ucloudbiz/16

iv. http://cafe.naver.com/ucloudbiz/17

D. 트래픽 수시 점검 및 이벤트 알람 설정

i. 해킹 등을 통해 악성코드에 감염된 VM 은 다량의 트래픽을 발생시킵니다. 계정의 outbound 트래픽을 수시로 점검하여 비정상 트래픽 유발 여부 확인해야 합니다.

ii. (콘솔 > ucloud server > 네트워크 트래픽 통계)에서 일간/주간 트래픽 통계 조회 및 알람을 관리할 수 있습니다.

iii. ucloud watch 서비스를 통해 VR outbound 트래픽에 대한 임계치 설정 및 모니터링을 할 수 있습니다.

iv. 모니터링 항목 :

(agentless, default) VM/VR 의 CPU, Disk Read/Write, Network In/Out, LB 의 Requests, Throughput, Connections

(agent 설치 후 추가 제공) Linux : CPULoad, RootFileSystemUsage, DeviceReadOPS, DeviceWriteOPS, MemoryUsage, ProcessList. Windows: CPULoad, RootFileSystemUsage, MemorySwqpUsage, ProcessList

v. Agent 다운로드: https://ucloudbiz.olleh.com/portal.portalinfo2.html "ucloud watch agent" 메뉴에서 다운로드 가능합니다.

vi. 연속 n 회 주기 동안 특정 모니터링 값이 x 값을 ***할 경우 경보 발생하도록 설정할 수 있습니다. (※ *** : 클 때, 크거나 같을 때, 작을 때, 작거나 같을 때)

vii. 알람은 관리자에게 이메일/SMS 로 통보 또는 오토스케일링을 사용하실 수 있습니다.

E. ucloudbiz 포탈 계정 보호

i. 포탈 계정의 비밀번호를 주기적으로 변경 및 계정 로그인 시 OTP 설정하실 것을 권고 드립니다.

ii. 계정 로그인 시 OTP 설정 방법: (포탈 > 내 정보 관리 > 개인정보 > 로그인 방식 선택) ※ 해외사용자를 위해 SMS 외 이메일 인증도 지원합니다.

F. ucloudbiz 고객 권고 사항 (공지사항) 협조/준수

i. 수시로 발생하는 보안 사고, 신규 취약점 발견에 따른 업데이트 등 보안 이벤트 발생 시, 사용자의 조치가 필요한 사항을 수시로 ucloudbiz 포탈이나 메일을 통해 고객께 전달 드립니다.

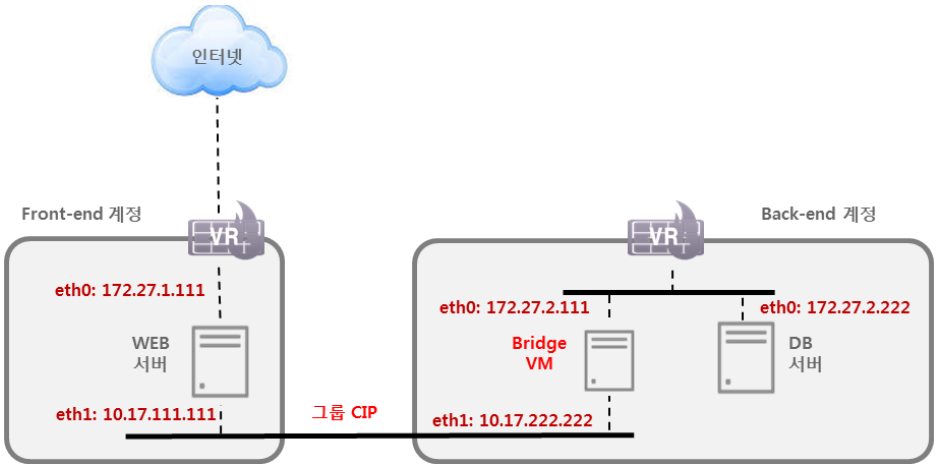
ii. ucloudbiz 포탈이나 메일을 통해 안내해 드리는 공지사항을 참고하시고 협조/준수 부탁 드립니다.

4. 망 분리를 통한 보안 강화

고객 별 2 개의 zone(공인 인터넷망과 연결된 Public zone(DMZ), 물리적으로 인터넷망과 차단되어 내부 사설 통신만 가능한 Private zone)을 분리하여 제공해 드립니다. Zone 별로 각 방화벽이 있으며(Pub-FW, Inter-FW, Priv-FW), Public(DMZ) zone 은 IPS 로 관제합니다.

A. 계정 분리

i. Front-end 서버를 수용할 계정과, Back-end 서버를 수용할 계정을 별도로 구성하여 계정을 분리하시면 보안성을 높일 수 있습니다.



<그림 7. Front-End 와 Back-End 계정 분리>

ii. 보안성 뿐만 아니라 편의성도 고려하여, 분리하신 두 개의 계정을 하나의 그룹계정으로 연결하여 사용하실 수 있습니다.

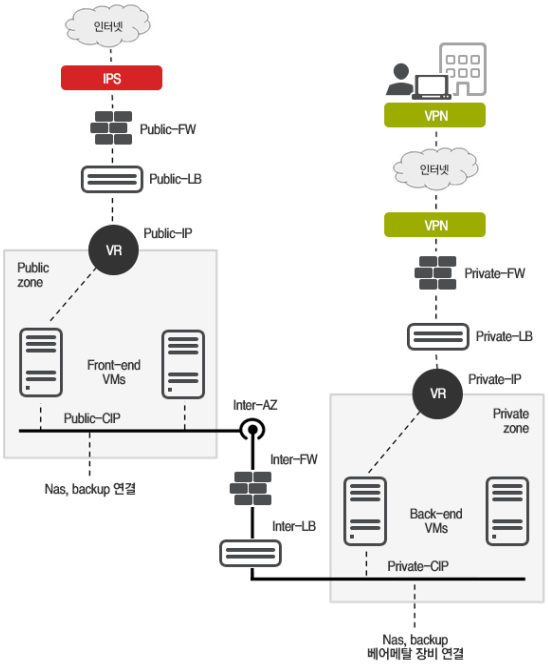
iii. 두 개의 계정을 하나의 그룹계정으로 연결 (https://ucloudbiz.olleh.com/portal/portal.myinfo.group.html)

iv. 계정간 그룹 CIP 생성 : 계정간 통신채널 개설 (https://ucloudbiz.olleh.com/manual/CIP(Cloud%20Internal%20Path)_user_guide.pdf)

B. 기본으로 제공되는 Public Cloud 의 두 개 zone 외에도, G-Cloud 와 Enterprise Cloud 를 제공합니다.

C. Enterprise Cloud 사용

i. Enterprise Cloud(zone)은 외부 서비스망이 연결된 public 영역, 물리적으로 외부와 차단되어 내부 통신만 가능한 private 영역 2 개로 분리되어 제공됩니다.



<그림 8. Enterprise Cloud 의 Public zone 과 Private zone 구성도>

ii. Enterprise Cloud 에 대한 자세한 사항은 아래 링크를 참고하시기 바랍니다.

iii. https://ucloudbiz.olleh.com/portal/ktcloudportal.epc.productintro.enterprise.html

https://gov.ucloudbiz.olleh.com/portal/ktcloudportal.epc.introduction.html