시스템 보안 강화 가이드

V1.3 (2015.9)

KT ucloud biz 총판 / 아마존 AWS partner

Ncloud24

www.ncloud24.com, 엔클라우드24

1. VR/VM 레벨에서의 보안 강화 방안

1.1 VR 보안 설정

○ 포트포워딩 설정 시, public port 는 well-known port 를 피해서 설정

- 외부로 노출되는 public port 를 알려진 port 로 설정 시 (ex. web 서비스에 80 포트, ssh 접속 IP 에 22 포트), port scan 에 의한 공격에 취약하게 됨
- VR 이 있는 NAT 구조이므로, 임의의 public port 와 실제 사용될 private port 를 다르게 포트포워딩 하는 것이 유리 (ex. SSH : public 10001 = private 22)

○ VR 방화벽 기능 사용

- VR 의 네트워크 기능을 보면 접근하는 client 의 IP 대역(CIDR)을 제한할 수 있는 기능이 있음 (포탈 > 클라우드콘솔 > ucloud server > 네트워크 > IP 선택 > Firewall)
- 기본적으로 포트포워딩이 추가된 포트에 대해 0.0.0.0/0(모두 허용)으로 설정되므로 SSH 와 같은 critical 한 포트는 client IP 로 제한 필요

1.2 VM 보안 설정

○ SSH key 를 통한 로그인 설정

- http://cafe.naver.com/ucloudbiz/115 참고

○ VM 비밀번호 강화

- https://ucloudbiz.olleh.com/manual/Security_Password_change.pdf 참고

○ Linux VM 의 fail2ban 활용

- https://ucloudbiz.olleh.com/manual/Security_fail2ban.pdf 참고

○ Linux VM 의 root 로그인 제한

- https://ucloudbiz.olleh.com/manual/Security_sshd_config_root_login_Limited.pdf 참고

○ Google Authenticator 를 이용한 Two-Factor OTP Login

- http://cafe.naver.com/ucloudbiz/129 참고

○ VM 의 자체 방화벽 활성화

○ 보안 솔루션 혹은 서비스 사용

- 서버 백신, 웹 쉘 방어, DB 보안 등

○ 보안성 검사 수행

- KISA 인터넷침해대응센터(http://www.krcert.or.kr)에서 제시하는 각종 가이드 활용

2. 시스템 레벨에서의 보안 강화 방안

2.1 아키텍처 구성

○ Backend 시스템 VM 의 포트포워딩 미설정 혹은 계정 분리 (CIP 통신)

- 시스템의 backend 시스템 VM(ex. DB 서버)의 경우, 포트포워딩을 하여 외부로 노출시키는 것을 지양
- Frontend VM 과 사설 IP(혹은 CIP)를 통하여 통신만 가능하도록 구성

○ 관리용 OpenVPN 사용

- 별도 OpenVPN 서버를 두어서 외부에서 직접 서버 접근이 불가하면서 접근 루트를 일원화 함
- 설정 참고 : https://ucloudbiz.olleh.com/manual/OpenVPN_setting_Guide.pdf, http://cafe.naver.com/ucloudbiz/16, http://cafe.naver.com/ucloudbiz/17

○ 보안 관련 엔클라우드 24 상품 활용

- 웹 방화벽(WAF) : HTTP/HTTPS 기반의 웹 공격을 차단하는 웹 방화벽, SQL injection, Cookie 변조, SSL 검사 등

2.2 기타 시스템 레벨 보안

○ 개발 계정과 상용 계정의 분리

○ 트래픽 수시 점검

- 해킹 당해 좀비 역할을 하는 VM 에서는 outbound 트래픽이 급증하는 현상을 보이므로, outbound 트래픽이 급증하지 않는지 수시 점검
- cloud watch 서비스를 이용하여 VR outbound 트래픽에 대한 임계치 알람 설정

○ 엔클라우드 24 고객 권고 사항 (공지사항) 협조/준수

3. 망분리를 통한 보안 강화

3.1 Enterprise Cloud 사용

○ Enterprise cloud(zone)는 외부 서비스망이 연결된 public 영역, 물리적으로 외부와 차단되어 내부 통신만 가능한 private 영역 2 개로 분리되어 있음

○ https://www.ncloud24.com/goods/enterprice_cloud.php

3.2 일반 zone 에서 망 분리 방안

○ 계정 분리 : Frontend 서버를 수용할 계정과 Backend 서버를 수용할 계정을 별도로 구성

- Step 1. 두 계정을 하나의 그룹 계정으로 연결
- Step 2. 계정 간 그룹 CIP 생성 (계정 간 통신채널 개설)

○ Bridge VM 구성

- Backend 계정에 Linux OS 로 Bridge VM 생성
- Bridge VM 이 Frontend 계정과 Backend 계정 사이의 방화벽 역할을 하도록 구성 (Linux 의 iptables 기능)
- 인가되지 않은 패킷은 drop 처리하고 로그를 남김
- http://cafe.naver.com/ucloudbiz/70