

중소기업 네트워크 장비 보안점검 안내서



과학기술정보통신부



한국인터넷진흥원



인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

CONTENTS

I. 개요	1
1. 배경	1
2. 안내서 목적 및 구성	2
II. 네트워크 장비 보안 점검	3
1. 보안 점검 항목	4
2. 장비 콘솔 연결 절차	5
3. 보안 점검 절차	6

본 매뉴얼의 내용에 대해 한국인터넷진흥원의 허가 없이 무단전재
및 복사를 금하며, 위반 시 저작권법에 저촉될 수 있습니다.

제1장

개요

1. 배경

최근 몇 년 사이에 코로나19, 효율성 증대 등의 이유로 대면 서비스의 비대면화와 근무 형태 변경 등이 이루어졌고, 기업에서는 이러한 환경 변화에 의한 수요를 충족시키고자 효율적 네트워크를 중심으로 짧은 시간 내 인프라를 구축하거나 확장하는 등 신속하게 비대면 업무 환경을 적용 하였다.

그러나 충분한 보안성 검토가 이뤄지지 못한 상황에서의 인프라 변경은 잠재적인 보안 취약점이 존재할 수 있으며 이로 인해 다양한 해킹 공격에 쉽게 노출될 수 있어 주의가 필요하다.

네트워크 장비는 고객에게 서비스를 제공하거나, 기업 내부 시스템 운영을 위한 인프라 구성 장비 중 필수 장비이지만 일반적으로 초기 인프라 구축 후 점검 및 설정 변경 없이 장기간 운영되어, 서버나 서비스에 비해 상대적으로 관리가 소홀한 경우가 많다.

하지만 최근 러시아, 중국 등 국가를 배후로 한 해킹 그룹이 네트워크 장비의 취약점을 공격하는 사례가 증가하고 있으며, 네트워크 장비를 대상으로 침해사고 발생하는 경우 연결된 모든 서비스의 제공이 중단되는 등 피해 파급도가 높기 때문에 기업에서는 서비스의 가용성을 보장하기 위해 네트워크 장비도 중요하게 관리해야 한다.

한국인터넷진흥원(KISA)에서는 보호나라 홈페이지(www.boho.or.kr)를 통해 라우터, 스위치 제품 관련 업데이트, 주의 권고문을 지속적으로 발표하여 네트워크 장비에 대한 보안 수준을 강화할 것을 권고하고 있으며, 이와 함께 중소기업의 보안수준 제고를 위해 네트워크 장비의 보안 점검 방안을 알리고자 「중소기업 네트워크 장비 보안점검 안내서」를 발간하였다.

이 안내서는 중소기업에서 네트워크 장비를 운영함에 있어서 지켜야하는 계정관리, 접근관리 등 최소한의 보안 설정 점검 항목을 중점적으로 다루고 있으며 정보보호 인력이 부족한 중소기업에서도 네트워크 장비의 취약 요인을 스스로 점검하고 관리할 수 있도록 명령어를 포함하여 상세하게 기술하였다. 더 많은 항목으로 관리를 하고자 하는 기업은 「주요 정보통신 기반시설 기술적 취약점 분석 평가 상세 가이드」 등의 가이드를 참고할 수 있다.

본 안내서를 통해 기업의 보안수준을 강화하고, 안정적인 서비스 제공뿐만 아니라 이용자에게 안전한 인터넷 환경을 제공할 수 있기를 바란다.

2. 안내서 목적 및 구성

목적	중소기업에서 운영 중인 라우터, 스위치 등 네트워크 장비의 보안 설정 적용으로 안전한 네트워크 장비 운영 및 침해사고 예방
대상	네트워크 장비를 운영 중인 중소기업
범위	본 안내서는 CISCO, Juniper 장비를 기준으로 작성되었으며 모델, 펌웨어 버전, 구성된 설정에 따라 명령어 적용방법이 다를 수 있음
구성	<p>I. 개요</p> <ol style="list-style-type: none"> 1. 배경 2. 안내서 목적 및 구성 <p>II. 네트워크 장비 보안 점검</p> <ol style="list-style-type: none"> 1. 보안 점검 항목 2. 장비 콘솔 연결 절차 3. 보안 점검 절차 <ul style="list-style-type: none"> · 계정관리 · 접근관리 · 패치관리 · 보안관리 · 로그관리 · 기능관리

제2장

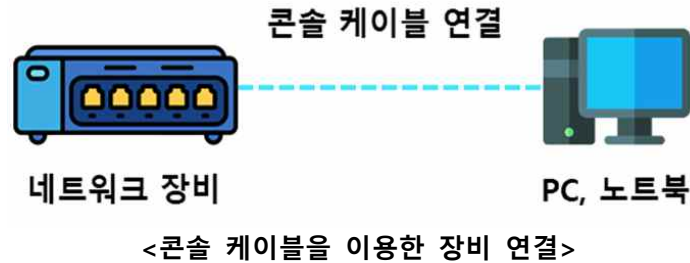
네트워크 장비 보안 점검

1. 보안 점검 항목

대상 장비	구분	항목 번호	점검 항목
스위치, 라우터	계정관리	1	패스워드 설정
		2	패스워드 복잡성 설정
		3	암호화된 패스워드 사용
	접근관리	4	VTY 사용 시 안전한 프로토콜 사용
		5	VTY 접근통제(ACL) 적용
		6	세션 타임아웃 설정
	패치관리	7	최신 보안패치 및 벤더 권고 적용
	보안관리	8	스푸핑 방지 필터 설정
		9	서비스 거부 공격 차단 필터 설정
		10	ICMP Unreachable, ICMP Redirect 차단
	로그관리	11	로그 활성화 및 버퍼 크기 설정
	기능관리	12	미사용 인터페이스 비활성화
		13	불필요한 서비스 비활성화
		14	취약한 서비스 비활성화

2. 장비 콘솔 연결 절차

1) 콘솔 케이블을 이용한 네트워크 장비 연결 방법



- ① 라우터, 스위치 장비 외부에 존재하는 콘솔 포트에 콘솔 케이블*을 연결하여 PC, 노트북과 직접 연결
 * 콘솔 연결을 위해 RJ45 to DE9(D-sub9) 케이블을 사용하거나, 연결하려는 PC, 노트북에 직렬 포트(시리얼 포트)가 없는 경우, DE9 to USB 케이블과 결합하여 USB로 연결하여 사용



<RJ-45 to DE9 케이블>

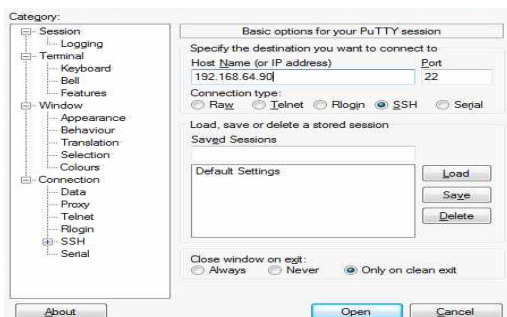


<DE9 to USB 케이블>

- ② 터미널 프로그램(putty, 하이퍼터미널 등)을 사용하여 Serial 통신 연결*
 - Serial 통신 연결 시 전송속도, 흐름제어 등 관련 설정은 벤더사별, 제품별 설정이 상이하므로 제품별 설정 확인 필요
 * 예) Baud rate 9600, Flow control None, Data 8, Parity None, Stop bits 1

2) 원격터미널을 이용한 네트워크 장비 연결 방법

라우터, 스위치 장비에 원격 터미널(Telnet, SSH) 접속이 허용된 경우, putty 등과 같은 원격 터미널 접속 소프트웨어를 활용하여 원격 접속

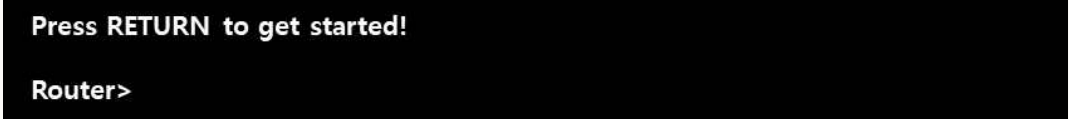
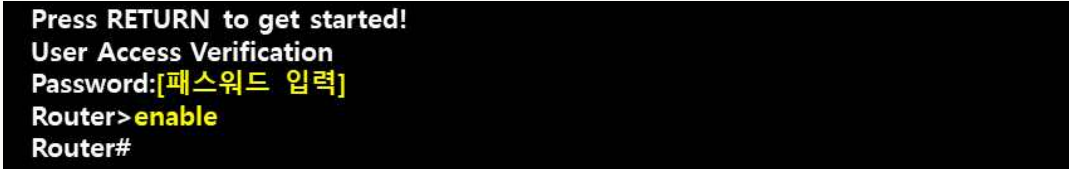
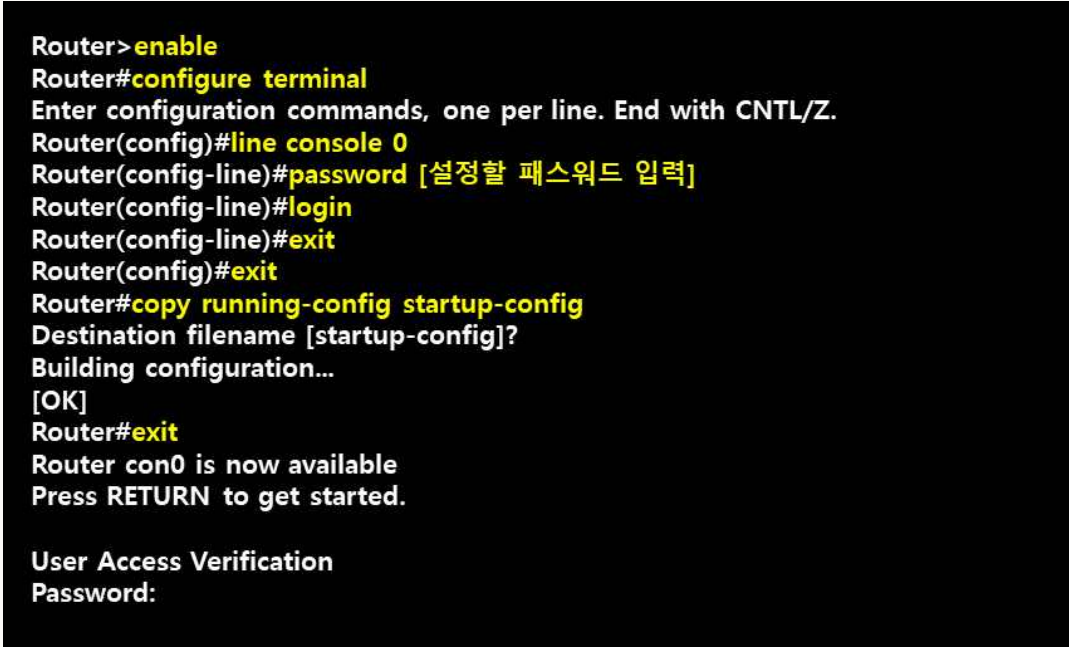


<원격 터미널 접속 설정>



<원격 터미널 접속 화면>

3. 보안 점검 절차

계정관리	1. 패스워드 설정
보안 위협	
비인가자가 웹 검색을 통해 장비의 기본 패스워드를 확인하여 무단으로 접근 및 임의로 트래픽의 경로를 변경하거나 통신 장애를 발생시킬 수 있는 위험이 존재하므로, 기본 패스워드는 변경 필요	
판단 기준	
양호	기본 패스워드를 변경하거나 패스워드를 설정하여 사용
취약	기본 패스워드 사용 또는 패스워드 미설정으로 사용
CISCO	
점검 방법	1. Console : 콘솔 연결 시 User Access Verification 단계 패스워드 입력 요구 확인 
	2. Privileged mode : User mode에서 enable 명령어 입력 시 패스워드 입력 요구 확인 
조치 방법	1. Console User Access Verification 단계 패스워드 인증 설정 적용 

CISCO	
조치 방법	<p>2. Privileged mode 권한 상승 시 password 인증 설정 적용</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#enable secret [설정할 패스워드 입력] Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#exit Router con0 is now available Press RETURN to get started. User Access Verification Password:[패스워드 입력] Router>enable Password: </pre>
Juniper	
점검 방법	<p>■ Console : 기본 root 계정 접속 시 패스워드 입력 요구 확인</p> <pre> Amnesiac (ttyu0) login: root --- JUNOS 12.3R12.4 built 2016-01-20 04:27:51 UTC root@:RE:0% </pre>
조치 방법	<p>■ Console 연결 시 패스워드 인증 설정 적용</p> <p>※ plain-text-password를 사용하여도 자동 암호화 됨(auto-encrypted)</p> <pre> Amnesiac (ttyu0) login: root --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@:RE:0% cli root> configure Entering configuration mode The configuration has been changed but not committed [edit] root# set system root-authentication plain-text-password New password : [패스워드 입력] Retype new password: [패스워드 입력] [edit] root# commit Commit complete </pre>

계정관리	2. 패스워드 복잡성 설정
보안 위협	
취약한 패스워드를 사용 중인 경우 비인가자의 무작위 대입 공격 시 짧은 시간 안에 계정이 탈취될 위험이 존재하므로, 패스워드 복잡성 정책을 설정하여 복잡성을 만족하는 패스워드 사용 필요	
판단 기준	
양호	복잡성 정책을 설정하거나, 복잡성 설정 기능이 없는 경우 영문 대문자, 소문자, 숫자, 특수문자 복잡성을 만족한 패스워드 사용
취약	쉽게 유추할 수 있는 패스워드 사용 또는 취약한 패스워드* 사용 * 예) cisco, juniper, admin, qwert123, 12345, pass1 등
공통	
점검 방법	<p>■ 영문(대문자, 소문자), 숫자, 특수문자를 사용한 복잡성 만족 패스워드 사용여부 확인</p> <ol style="list-style-type: none"> 1. 사용자 계정과 동일한 패스워드 사용 금지 2. 개인 신상 및 부서, 기업 명칭과 관계있는 패스워드 사용 금지 3. 일반 사전에 등록된 단어의 사용 금지 4. 동일한 단어 및 숫자 반복하여 사용 금지 5. 사용된 패스워드는 재사용 금지 6. 동일한 패스워드를 여러 사람 공유하여 사용 금지 7. 연속된 문자 및 숫자를 사용 금지
CISCO	
조치 방법	<p>■ 패스워드의 최소 길이 설정 적용(※ IOS 버전에 따라 지원되지 않는 버전 존재)</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#configure terminal Router(config)#security passwords min-length ? <0-16> Minimum length of all user/enable passwords Router(config)#security passwords min-length 8 Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] </pre>

Juniper

■ 패스워드의 최소길이, 영문 대·소문자, 특수문자 등 복잡도 설정 적용

조치
방법

```

Amnesiac (ttyu0)

login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.4 built 2016-01-20 04:27:51 UTC

root@RE:0% cli
root> configure
Entering configuration mode

[edit]
root# set system login password ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
change-type            Password change type
format                Encryption method to use for password
maximum-length         Maximum password length for all users (20..128)
minimum-changes        Minimum number of changes in password
minimum-length         Minimum password length for all users (6..20)
minimum-lower-cases    Minimum number of lower-case class characters in password
minimum-numeric        Minimum number of numeric class characters in password
minimum-punctuations   Minimum number of punctuation class characters in password
minimum-upper-cases    Minimum number of upper-case class characters in password

root# set system login password minimum-length 8          ## 최소 8글자 이상
[edit]
root# set system login password minimum-upper-cases 1     ## 대문자 1글자 이상
[edit]
root# set system login password minimum-lower-cases 1     ## 소문자 1글자 이상
[edit]
root# set system login password minimum-punctuations 1    ## 특수문자 1글자 이상
[edit]
root# set system login password minimum-numeric 1        ## 숫자 1글자 이상
[edit]
root# commit
Commit complete

```

계정관리	3. 암호화된 패스워드 사용
보안 위협	
비인가자가 장비에 접근하여 설정 확인 시 장비의 계정 및 패스워드를 평문으로 열람이 가능하여 관리자 계정 탈취 위험이 존재하므로, 패스워드 암호화 기능을 활용하여 패스워드 암호화 저장 필요	
판단 기준	
양호	설정 조회 시 암호화된 패스워드 출력
취약	설정 조회 시 평문 패스워드 출력
CISCO	
점검 방법	<p>■ 설정 확인 명령어를 통해 설정된 패스워드가 평문으로 출력되는지 여부 확인</p> <p>- [1. enable secret], [2. username secret], [3. password-encryption] 서비스 확인</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#show running-config Building configuration... Current configuration : 1099 bytes ! version 12.4 no service password-encryption hostname Router enable password Assithepriv12() ~~~~중략~~~~ username admin password 0 adminpassword12#\$ ~~~~중략~~~~ line con 0 password co158283@#\$cis </pre>
조치 방법	<p>1. enable secret(암호화) 설정 및 기존 평문 패스워드 설정 삭제</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#enable secret [설정할 패스워드 입력] Router(config)#no enable password ## 기존 패스워드 삭제 Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#show running-config Building configuration... Current configuration : 1146 bytes ! version 12.4 no service password-encryption ! hostname Router ! enable secret 5 \$1\$mERr\$zvdpcAgaye5ZbJa67S.Aq0 </pre>

CISCO

2. username secret(암호화) 설정 및 기존 평문 패스워드 설정 삭제

```

User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no username admin          ## 기존 계정 삭제
Router(config)#username admin secret [설정할 패스워드 입력]
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#show running-config
Building configuration...
Current configuration : 1117 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
enable secret 5 $1$mERr$zvdpcAgaye5ZbJa67S.Aq0
~~~~중략~~~~
username admin secret 5 $1$mERr$NeyFf/t7M4QrX1gYyC8wU1

```

조치
방법

3. password-encryption 설정

※ 설정파일(running-config/startup-config)에 존재하는 평문 패스워드를 암호화하여 저장

```

User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#show running-config
Building configuration...
Current configuration : 1127 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
enable secret 5 $1$mERr$zvdpcAgaye5ZbJa67S.Aq0
~~~~중략~~~~
username admin secret 5 $1$mERr$NeyFf/t7M4QrX1gYyC8wU1
~~~~중략~~~~
line con 0
password 7 080A455D084954464A4A

```

Juniper	
점검 방법	<ul style="list-style-type: none"> ■ “show configuration system” 설정 확인을 통해 패스워드 평문 노출 여부 확인 <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@:RE:0% cli root> show configuration system time-zone Asia/Seoul; root-authentication { encrypted-password "\$1\$QMC70fEw\$CLjtyr7QGgshml0NNnsF6/"; ## SECRET-DATA </pre>
조치 방법	<ul style="list-style-type: none"> ■ 기본적으로 패스워드를 암호화하여 저장

접근관리	4. VTY 사용 시 안전한 프로토콜 사용
보안 위협	
평문 원격 터미널 서비스(Telnet)를 사용하여 네트워크 장비에 접근 시 스니핑 공격에 의해 관리자 계정 정보, 사용 명령어가 비인가자에게 유출될 위험이 존재하므로, 평문으로 통신하는 원격 터미널 서비스 비활성화 및 암호화 프로토콜을 사용한 원격 터미널 서비스(SSH) 사용 권고	
판단 기준	
양호	원격 터미널(VTY) 접근 시 암호화 프로토콜(SSH)을 이용한 접근만 허용하는 경우
취약	원격 터미널(VTY) 접근 시 평문 프로토콜(Telnet)을 이용한 접근을 허용하는 경우
CISCO	
점검 방법	<p>■ 암호화 프로토콜(SSH) 활성화 여부 확인</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#show ip ssh SSH Disabled - version 1.99 %Please create RSA keys (of atleast 768 bits size) to enable SSH v2. Authentication timeout: 120 secs; Authentication retries: 3 </pre>
	<p>1. SSH 사용을 위한 계정 생성</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#configure terminal Router(config)#username [계정명] secret [비밀번호] ## 계정 생성 Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#show running-config Building configuration... Current configuration : 1147 bytes ! version 12.4 ! ~~~중략~~~ username vulntest secret 5 \$1\$qERa\$V68xEP1Tn6ZS4rrRk1zf28 </pre>

CISCO

2. 암호화 프로토콜(SSH)을 사용한 VTY 설정

- host name, domain name 지정 및 암호화 key 생성, SSH version 및 옵션 설정

```
User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname [호스트네임]      ## 호스트네임 지정 필요, ex) R1
R1(config)#ip domain-name [도메인네임]    ## 도메인네임 지정 필요, ex) R1, R1.co.kr
R1(config)# crypto key generate rsa

The name for the keys will be: [호스트네임].[도메인네임]
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 2048    ## 2048 권고
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)# ip ssh time-out [0-120초]      ## interval 타임아웃 시간
R1(config)# ip ssh version 2              ## ssh 버전
R1(config)# ip ssh authentication-retries 3 ## 인증 실패시 재시도 횟수
R1(config)# line vty 0 4
R1(config-line)# transport input ssh       ## vty 접속 시 ssh 허용 설정
R1(config-line)# login local               ## vty 접속 시 local 계정 인증
R1(config-line)# exit
R1(config)# exit
R1#copy running-config startup-config

Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R1#
```

Juniper

■ telnet, ssh 서비스 활성화 여부 확인

점검
방법

```
Amnesiac (ttyu0)
login: root
Password: [패스워드 입력]
--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@RE:0% cli
root> show configuration system services
telnet;
dhcp {
  traceoptions {
    file dhcp_logfile;
    level all;
    flag all;
  }
}
```

Juniper

- 암호화 프로토콜(SSH)을 사용한 VTY 설정
 - SSH 서비스 활성화 및 Telnet 서비스 비활성화

조치
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]
--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@RE:0% cli
root> show configuration system services
telnet;
dhcp {
    traceoptions {
        file dhcp_logfile;
        level all;
        flag all;
    }
}
root> configure
Entering configuration mode
[edit]
root# set system services ssh                ## ssh 서비스 활성화
[edit]
root# set system services ssh protocol-version v2    ## ssh 버전 설정
[edit]
root# delete system services telnet            ## telnet 비활성화
root# commit
Commit complete

root# exit
Exiting configuration mode

root> show configuration system services
ssh {
    protocol-version v2;
}
dhcp {
    traceoptions {

```

접근관리	5. VTY 접근통제(ACL) 적용						
보안 위협							
비인가자가 장비 접근이 허용되어 장비를 대상으로 무작위 대입 공격과 같은 공격 시도가 가능하며, 관리자 권한 탈취 시 네트워크 설정 변경을 통해 데이터의 유출 및 가용성 저하 등의 위험이 존재하므로, 관리자가 사용하는 특정 IP로 접근통제 적용 필요							
판단 기준							
양호	가상 터미널(VTY)에 접근을 제한하는 ACL정책 적용						
취약	가상 터미널(VTY)에 접근을 제한하는 ACL정책 미적용						
CISCO							
점검 방법	<p>■ VTY에 Access-list 설정 여부 확인</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#show running-config ~~~ 중략 ~~~ ! line vty 0 4 login local transport input ssh ! ! end </pre>						
참고 사항	<p>■ 보안을 고려하여 원격 터미널을 통한 접근을 원칙적으로 금지하나, 부득이하게 VTY를 통해 접근이 필요한 경우 지정한 시스템에서만 접근할 수 있게 통제하여야 함</p> <p>■ Cisco의 Access-list(ACL), Juniper firewall filter는 위에서 부터 순차로 조건을 확인하여, 다수 정책이 존재할 경우 많은 자원을 소모하게 되어 장비 성능에 영향을 줄 수 있음</p> <p>■ 추후 침해사고 발생 시 원인추적을 위하여 로그 기능을 지원하는 경우 적용 권고 ※ 제품별, 장비별 제공 기능에 따라 로그 기능을 지원하지 않는 경우가 존재할 수 있음</p> <p>■ Access-list 관련 참고 사항</p> <ul style="list-style-type: none"> · Access-list설정은 주로 standard와 extended 방식을 많이 사용 · Access-list는 위에서부터 아래로 순서대로 조건을 확인 · Access-list는 정책 마지막에 deny any 추가 필요 <table border="1"> <thead> <tr> <th>Standard</th><th>Extended</th></tr> </thead> <tbody> <tr> <td>Access-list 번호 1-99번 또는 특정 이름 사용</td><td>Access-list 번호 100-199번 또는 특정 이름 사용</td></tr> <tr> <td>출발지 주소 기반 접근 제어</td><td>출발지, 목적지 주소, 프로토콜 기반 접근 제어</td></tr> </tbody> </table>	Standard	Extended	Access-list 번호 1-99번 또는 특정 이름 사용	Access-list 번호 100-199번 또는 특정 이름 사용	출발지 주소 기반 접근 제어	출발지, 목적지 주소, 프로토콜 기반 접근 제어
Standard	Extended						
Access-list 번호 1-99번 또는 특정 이름 사용	Access-list 번호 100-199번 또는 특정 이름 사용						
출발지 주소 기반 접근 제어	출발지, 목적지 주소, 프로토콜 기반 접근 제어						

CISCO	
조치 방법	<p>■ 장비 접근이 필요한 관리자IP, IP 대역에 대해서만 접속을 허용 하도록 Access-list 설정</p> <pre> Press RETURN to get started! User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#configure terminal Router(config)#access-list 1 permit 192.168.0.11 Router(config)#access-list 1 deny any Router(config)#line vty 0 4 Router(config-line)#access-class 1 in Router(config-line)#exit Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#show access-lists Standard IP access list 1 10 permit host 192.168.0.11 (2 match(es)) 20 deny any (10 match(es)) Router#show running-config ~~~ 중략 ~~~ line vty 0 4 access-class 1 in login local transport input ssh </pre>
Juniper	
점검 방법	<p>■ firewall filter 설정 및 loopback 인터페이스 적용 여부 확인</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@:RE:0% cli Entering configuration mode root> show configuration firewall root> show configuration interfaces lo0 </pre>

Juniper

- 장비 접근이 필요한 관리자IP 또는 대역에 대해서만 접속을 허용 하도록 firewall 설정

조치
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC

root@RE:0% cli
root> configure
Entering configuration mode

## 관리자 IP, 그룹 지정 < >안의 내용은 이해를 돕기 위해 예시로 임의 지정
root#set policy-options prefix-list <ssh_admin> <관리자 IP주소 또는 대역/CIDR>

## 정책(filter) 생성
root#set firewall family inet filter <mgt> term <ssh_permit> from source-
    prefix-list <ssh_admin>
root#set firewall family inet filter <mgt> term <ssh_permit> from protocol tcp
root#set firewall family inet filter <mgt> term <ssh_permit> from destination-port ssh
root#set firewall family inet filter <mgt> term <ssh_permit> then accept
root#set firewall family inet filter <mgt> term <ssh_deny> from source-address
    0.0.0.0/0
root#set firewall family inet filter <mgt> term <ssh_deny> from protocol tcp
root#set firewall family inet filter <mgt> term <ssh_deny> from destination-port ssh
root#set firewall family inet filter <mgt> term <ssh_deny> then discard

## lo0 인터페이스에 정책 적용
root#set interfaces lo0 unit 0 family inet filter input <mgt>
root# commit
commit complete

[edit]
root# run show configuration interfaces lo0
unit 0 {
    family inet {
        filter {
            input mgt;
        }
    }
}

```


접근관리	6. 세션 타임아웃 설정
보안 위협	
관리자 부재 시 비인가자가 네트워크 장비 터미널에 접속된 컴퓨터를 통해 네트워크 장비 설정 변경 등의 행위를 할 수 있는 위험이 존재하므로, 관리자의 부재를 대비하여 세션 만료 설정 적용 필요	
판단 기준	
양호	Session Timeout 시간을 기관 정책에 맞게 설정한 경우(5분이하 권고)
취약	Session Timeout 시간을 기관 정책에 맞게 설정하지 않은 경우
CISCO	
점검 방법	<p>■ 각 line의 exec-timeout 설정 확인</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#show running-config ~~~ 중략 ~~~ line con 0 login line aux 0 ! line vty 0 4 login local transport input ssh </pre>
조치 방법	<p>■ Console, AUX 및 VTY에 대한 Session Timeout 조치 방법(Timeout 5분 이내 설정 권고)</p> <pre> User Access Verification Password:[패스워드 입력] Router>enable Password:[패스워드 입력] Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#line con 0 Router(config-line)#exec-timeout 5 0 Router(config-line)#exit Router(config)#line vty 0 4 Router(config-line)#exec-timeout 5 0 Router(config-line)#exit Router(config)#line aux 0 Router(config-line)#exec-timeout 5 0 Router(config-line)#exit Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#show running-config ~~~ 중략 ~~~ line con 0 exec-timeout 5 0 ~~~중략~~~ line aux 0 exec-timeout 5 0 line vty 0 4 access-class 1 in exec-timeout 5 0 </pre>

Juniper	
점검 방법	<p>■ idle-timeout 설정 확인</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.4 built 2016-01-20 04:27:51 UTC root@RE:0%cli root> show configuration system login root> </pre>
조치 방법	<p>■ Console 접속 후 Session Timeout 조치 방법(Timeout 5분 이내 설정 권고)</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.4 built 2016-01-20 04:27:51 UTC root@RE:0%cli root> configure Entering configuration mode root# set system login class timeout idle-timeout 5 root# commit commit complete </pre>

패치관리	7. 최신 보안패치 및 벤더 권고 적용
보안 위협	
알려진 네트워크 장비의 결함이나 취약점을 통해 장애 발생 또는 관리자 권한 탈취가 가능하므로 벤더 패치 발표 시 보안성 강화 및 기능 향상을 위해 주기적인 업데이트 작업 수행 필요	
판단 기준	
양호	주기적으로 보안 패치 및 벤더 권고사항을 적용하는 경우
취약	주기적으로 보안 패치 및 벤더 권고사항을 적용하지 않는 경우
CISCO	
점검 방법	<p>■ 버전정보 확인 방법</p> <pre> User Access Verification Password:[패스워드 입력] Router>show version Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Wed 18-Jul-07 04:52 by pt_team ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1) ~~~종락~~~ </pre>
Juniper	
점검 방법	<p>■ 버전정보 확인 방법</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.4 built 2016-01-20 04:27:51 UTC root@:RE:0%cli root> configure Entering configuration mode root# show version ## Last changed: 2016-01-20 20:47:56 KST version 12.3R12.4; </pre>

공통

조치
방법

■ 패치 관리 방법

1. 패치 식별

- 네트워크 장비의 하드웨어, 소프트웨어, EOL, 패치 적용 현황을 문서화*하여 관리
* 예) 네트워크 장비 보안패치 관리대장 등
- 운영 중인 네트워크 장비의 보안 패치 및 벤더 권고사항을 입수

2. 패치 분석

- 취약점의 영향도와 발생 가능성을 분석하여 패치 적용 여부와 우선순위를 결정
- 패치 없이 네트워크 장비 설정 변경 등으로 해결이 가능한 경우 대체 조치를 수행

3. 패치 테스트

- 테스트베드 또는 시뮬레이션에서 운영 환경과 최대한 유사하게 테스트 환경 구축
※ GNS3 등과 같은 가상 에뮬레이션을 이용한 테스트 진행

* **GNS3(Graphical Network Simulation)** : 오픈 소스, 무료 소프트웨어로 가상과 실제 네트워크를 에뮬레이션, 구성, 테스트 문제해결을 목적으로 사용

- 패치가 식별한 문제를 해결하고 정상 동작하는지 체크리스트를 구성하여 검증

4. 패치 적용

- 패치 적용 전에 네트워크 장비의 이미지와 설정을 백업하여 복구지점을 생성
- 예비 장비를 보유한 경우, 운영 장비 설정과 패치를 예비 장비에 적용하여 운영 장비와 교체하고 운영 장비는 비상상황에 대비하여 일정기간 유지
- 패치 적용 후 모든 인터페이스와 중요 호스트로의 통신이 정상 동작하는지 확인

5. 보안패치 및 보안권보 정보제공 사이트

구분	보안패치 및 보안권고 정보제공 사이트
공통	<ul style="list-style-type: none"> • KISA 인터넷보호나라 & KrCERT - https://www.krcert.or.kr
	<ul style="list-style-type: none"> • KISA 사이버 보안 취약점 정보포털 - https://knvd.krcert.or.kr
	<ul style="list-style-type: none"> • 국가사이버안보센터 - https://www.ncsc.go.kr
Cisco	<ul style="list-style-type: none"> • Cisco OS 다운로드 사이트 - https://software.cisco.com/download/home
	<ul style="list-style-type: none"> • Cisco 보안 취약점 정보 사이트 - https://sec.cloudapps.cisco.com/security/center/home.x
Juniper	<ul style="list-style-type: none"> • Juniper OS 다운로드 사이트 - https://support.juniper.net/support/downloads/
	<ul style="list-style-type: none"> • Juniper 보안 취약점 정보 사이트 - https://advisory.juniper.net

보안관리

8. 스푸핑 방지 필터 설정

보안 위협

IP 스푸핑 기반 DoS 공격으로 네트워크 장비의 한계를 초과하는 트래픽이 인입되면 연결된 서비스의 정상적인 제공이 불가하므로, 라우팅이 불가능한 IP주소(사설 네트워크, 루프백 등 특수용도 IP) 인입 시 차단하도록 스푸핑 방지 필터링(Anti-Spoofing Filtering) 기능 적용 필요

판단 기준

양호

라우터 또는 보안장비에 스푸핑 방지 필터링을 적용한 경우

취약

라우터 또는 보안장비에 스푸핑 방지 필터링을 적용하지 않은 경우

참고 사항

■ 특수 용도 IP 주소 차단 (RFC 6890 참조)

IP 주소 대역	설명
0.0.0.0/8	자체 네트워크(This host on this network, RFC1122)
10.0.0.0/8	사설 네트워크(Private-Use, RFC1918)
127.0.0.0/8	루프백(Loopback, RFC1122)
169.254.0.0/16	링크 로컬(Link Local, RFC3927)
172.16.0.0/12	사설 네트워크(Private-Use, RFC1918)
192.0.2.0/24	예제 등 문서에서 사용(TEST-NET-1, RFC5737)
192.168.0.0/16	사설 네트워크(Private-Use, RFC1918)
224.0.0.0/4	멀티캐스트(Multicast, RFC5771)

■ Spoofing 설정 시 주의 사항

· 인터페이스에 Spoofing 차단 설정 시 해당 인터페이스를 통해 사설IP로 통신이 필요한 경우 해당 IP 대역은 제외하고 설정

· OSPF, EIGRP, BGP 등 라우팅 및 HSRP, VRRP등과 같이 multicast를 사용하는 경우 해당 멀티캐스트 IP 주소는 제외하고 설정

CISCO

■ IP Spoofing 방지용 ACL 설정 확인

User Access Verification

Password:[패스워드 입력]

Router>enable

Password:[패스워드 입력]

Router#show running-config

Building configuration...

Current configuration : 1391 bytes

!

~~~중략~~~

interface FastEthernet0/0

ip address 10.10.10.2 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0

## 인터페이스별 관련 ACL 존재 여부 검토

점검 방법

조치  
방법

#### ■ IP Spoofing 방지용 ACL 적용 방법

```

User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny ip 0.0.0.0 0.255.255.255 any
Router(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
Router(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
Router(config)#access-list 100 deny ip 169.254.0.0 0.0.255.255 any
Router(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
Router(config)#access-list 100 deny ip 192.0.2.0 0.0.0.255 any
Router(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
Router(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
Router(config)#access-list 100 permit ip any any
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#show running-config
Building configuration...
~~~중략~~~
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip access-group 100 in
duplex auto
speed auto
!
access-list 100 deny ip 0.0.0.0 0.255.255.255 any
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 169.254.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.0.2.0 0.0.0.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit ip any any

```

#### Juniper

점검  
방법

#### ■ IP Spoofing 방지용 ACL 설정 확인

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]
--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@:RE:0% cli
root> show configuration interfaces <인터페이스명>
unit 0 {
 family inet {
 address 192.168.0.100/24;
 }
}
root> show configuration firewall
family inet {
 term ssh_deny {
 from {
 source-address {
 0.0.0.0/0;
 }
 protocol tcp;
 destination-port ssh;
 }
 }
}

```

## 인터페이스별 관련 filter 존재 여부 확인

## firewall에 설정된 filter 확인

## Juniper

## ■ IP Spoofing 방지용 ACL 적용 방법

조치  
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@:RE:0% cli
root> configure
Entering configuration mode

정책(filter) 생성, < >안의 내용은 이해를 돕기 위해 예시로 임의 지정
root# set firewall family inet filter <spoofing> term <deny> from source-address 0.0.0.0/8
root# set firewall family inet filter <spoofing> term <deny> from source-address 10.0.0.0/8
root# set firewall family inet filter <spoofing> term <deny> from source-address 127.0.0.0/8
root# set firewall family inet filter <spoofing> term <deny> from source-address 169.254.0.0/16
root# set firewall family inet filter <spoofing> term <deny> from source-address 172.16.0.0/12
root# set firewall family inet filter <spoofing> term <deny> from source-address 192.0.2.0/24
root# set firewall family inet filter <spoofing> term <deny> from source-address 192.168.0.0/16
root# set firewall family inet filter <spoofing> term <deny> from source-address 224.0.0.0/4
root# set firewall family inet filter <spoofing> term <deny> then discard
root# set firewall family inet filter <spoofing> term <permit> then accept

차단 인터페이스에 정책 적용
root# set interfaces <인터페이스명> unit <유닛번호> family <parameter> filter input <filter>
root# commit
commit complete
root# exit
root> show configuration
Last commit: 2023-12-02 05:15:47 KST by root
version 12.3R12.4;
~~~중략~~~
interfaces {
  ge-0/0/1 {
    unit 0 {
      family inet {
        filter {
          input spoofing;
        }
        address 10.10.0.1/24;
      }
    }
  }
}
~~~중략~~~
firewall {
 family inet {
 filter spoofing {
 term deny {
 from {
 source-address {
 0.0.0.0/8;
 10.0.0.0/8;
 127.0.0.0/8;
 169.254.0.0/16;
 172.16.0.0/12;
 192.0.2.0/24;
 192.168.0.0/16;
 224.0.0.0/4;
 }
 }
 then {
 discard;
 }
 }
 term permit {
 then accept;
 }
 }
 }
}

```

|                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--|
| 보안관리                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 9. 서비스 거부 공격 차단 필터 설정                            |  |
| 보안 위협                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
| DDoS(Distributed Denial of Service)공격으로 인해 네트워크 및 시스템 리소스가 고갈되어 서비스 제공이 지연되거나 서비스 장애로 이어질 수 있으므로, 네트워크 장비 또는 DDoS 대응장비에 공격 방어 설정을 적용하여 피해 최소화 필요 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
| 판단 기준                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
| 양호                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 네트워크 장비에서 DDoS 공격 방어 설정을 하거나 DDoS 대응장비 사용        |  |
| 취약                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 네트워크 장비에서 DDoS 공격 방어 설정이 존재하지 않거나, DDoS 대응장비 미사용 |  |
| CISCO                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
| 점검<br>방법                                                                                                                                         | ■ 설정 조회를 통해 DDoS 방어 설정요소 확인                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                  |  |
|                                                                                                                                                  | <div>User Access Verification<br/>Password:[패스워드 입력]<br/>Router&gt;enable<br/>Password:[패스워드 입력]<br/>Router#show running-config<br/>show running-config<br/>Building configuration...<br/>Current configuration : 1859 bytes<br/>version 12.4<br/>!<br/>ip cef<br/>no ipv6 cef<br/>ip ssh version 2</div> ## DDoS 방어 관련 설정확인                                                                                                                                           |                                                  |  |
| Juniper                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                  |  |
| 점검<br>방법                                                                                                                                         | ■ 설정 조회를 통해 DDoS 방어 설정요소 확인                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                  |  |
|                                                                                                                                                  | <div>Amnesiac (ttyu0)<br/>login: root<br/>Password: :[패스워드 입력]<br/><br/>--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC<br/>root@RE:0% cli<br/>root&gt; show configuration<br/>## Last commit: 2023-12-02 05:33:07 KST by root<br/>version 12.3R12.4;<br/><br/>interfaces {<br/>  ge-0/0/0 {<br/>    unit 0 {<br/>      family inet {<br/>        address 192.168.0.100/24;<br/>      }<br/>    }<br/>  }<br/>  ge-0/0/1 {<br/>    unit 0 {</div> ## DDoS 방어 설정요소 확인 |                                                  |  |



| 공통                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |              |          |                                                                                                                                                          |                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 조치<br>방법                                                                                                                                                 | <p>■ 스푸핑 방지 필터링 등을 제외한 DDoS 공격 방어 설정은 DDoS 공격 발생 시 공격 유형과 상황을 고려하여 적용 필요</p> <p><b>1. ACL(Access Control List)</b></p> <ul style="list-style-type: none"> <li>- 스푸핑 방지 필터링을 사전 적용(8번 점검 항목)</li> <li>- DDoS 공격 유형에 따라 공격 대상 IP 주소, 프로토콜, 포트를 임시 차단</li> </ul> <p><b>2. Rate limiting</b></p> <ul style="list-style-type: none"> <li>- 특정 유형의 트래픽에 대역폭과 일정시간 동안 전송량을 제한</li> <li>- DDoS 공격 유형에 따라 UDP, ICMP, TCP SYN 패킷의 대역폭을 제한하여, 다른 서비스에 필요한 대역폭을 확보</li> <li>- 하드웨어 기반 전용모듈이 없는 경우 정책 수에 따라 라우터의 CPU 부하가 증가</li> </ul> <p><b>3. TCP Intercept</b></p> <ul style="list-style-type: none"> <li>- TCP SYN Flooding 공격으로부터 서버를 보호하며 Intercept 또는 Watch 모드로 설정</li> </ul> <p>※ Intercept 모드는 Watch 모드보다 라우터의 메모리와 CPU를 많이 사용</p> <table border="1"> <thead> <tr> <th>Intercept 모드</th><th>Watch 모드</th></tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전송하지 않고 라우터가 대신 SYN-ACK를 응답</li> <li>- 정상적으로 TCP 3-way Handshake가 완료되면 서버로 원래 SYN 패킷을 전송</li> </ul> </td><td> <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전달</li> <li>- 30초 안에 연결이 완료되지 않으면 서버에 RST를 전송하여 불완전 연결 상태 정리</li> </ul> </td></tr> </tbody> </table> | Intercept 모드 | Watch 모드 | <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전송하지 않고 라우터가 대신 SYN-ACK를 응답</li> <li>- 정상적으로 TCP 3-way Handshake가 완료되면 서버로 원래 SYN 패킷을 전송</li> </ul> | <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전달</li> <li>- 30초 안에 연결이 완료되지 않으면 서버에 RST를 전송하여 불완전 연결 상태 정리</li> </ul> |
| Intercept 모드                                                                                                                                             | Watch 모드                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |          |                                                                                                                                                          |                                                                                                                              |
| <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전송하지 않고 라우터가 대신 SYN-ACK를 응답</li> <li>- 정상적으로 TCP 3-way Handshake가 완료되면 서버로 원래 SYN 패킷을 전송</li> </ul> | <ul style="list-style-type: none"> <li>- SYN 패킷을 서버로 전달</li> <li>- 30초 안에 연결이 완료되지 않으면 서버에 RST를 전송하여 불완전 연결 상태 정리</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |              |          |                                                                                                                                                          |                                                                                                                              |

| 보안관리                                                                                                                                    | 10. ICMP Unreachable, ICMP Redirect 차단                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 보안 위협                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ICMP Unreachable를 차단하지 않으면 공격자가 시스템 운영 상태 정보를 스캔할 수 있으며, ICMP Redirect를 차단하지 않으면 특정 목적지로 가기 위해 고의적으로 패킷 경로를 변경하여 가로챌 수 있어 ICMP 차단 설정 필요 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 판단 기준                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 양호                                                                                                                                      | ICMP Unreachable, ICMP Redirect에 대해 차단하는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 취약                                                                                                                                      | ICMP Unreachable, ICMP Redirect에 대해 차단하지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CISCO                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 점검<br>방법                                                                                                                                | <p>■ 설정 조회를 통해 ICMP 차단 관련 설정 확인</p> <pre> User Access Verification Password:[패스워드 입력] Router&gt;enable Password:[패스워드 입력] Router#show running-config show running-config Building configuration... Current configuration : 1859 bytes ## no ip unreachablees 설정확인 ## no ip redirects 설정확인 </pre>                                                                                                                                                                                                                                                                                                                                                                                     |
| 조치<br>방법                                                                                                                                | <p>■ 사용 중인 Interface에 ICMP 차단 설정 진행</p> <pre> User Access Verification Password:[패스워드 입력] Router&gt;enable Password:[패스워드 입력] Router# config terminal Router(config)# interface &lt;인터페이스&gt; Router(config-if)# no ip unreachablees Router(config-if)# no ip redirects Router(config-if)# exit Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] Router#show running-config ~~~중략~~~ interface FastEthernet0/0 ip address 10.10.10.2 255.255.255.0 no ip redirects no ip unreachablees duplex auto speed auto ! interface FastEthernet1/0 ip address 192.168.1.1 255.255.255.0 duplex auto </pre> |

| Juniper  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 점검<br>방법 | <p>■ 설정 조회를 통해 ICMP 차단 관련 설정 확인</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력]  --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@RE:0% cli root&gt; show configuration          ## ICMP unreachable, redirects 설정 확인 ## Last commit: 2023-12-02 05:33:07 KST by root version 12.3R12.4;  interfaces {   ge-0/0/0 {     unit 0 {       family inet {         address 192.168.0.100/24;       }     }   } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 조치<br>방법 | <p>■ 사용 중인 Interface에 ICMP 차단 설정 진행</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력]  --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@RE:0% cli root&gt; configure Entering configuration mode  ## no-redirect 설정 root#set system no-redirects  ## icmp unreachable 차단 정책(filter) 생성 root#set firewall family inet filter &lt;icmp&gt; term &lt;deny&gt; from protocol icmp-type unreachable root#set firewall family inet filter &lt;icmp&gt; term &lt;deny&gt; then discard root#set firewall family inet filter &lt;icmp&gt; term &lt;permit&gt; then accept ## 차단 인터페이스에 정책 적용 root# set interfaces &lt;인터페이스명&gt; unit &lt;유닛번호&gt; family &lt;parameter&gt; filter input &lt;filter&gt; root# commit commit complete  [edit] root# show ## Last changed: 2023-12-02 06:30:37 KST version 12.3R12.4; system {   time-zone Asia/Seoul;   no-redirects;   root-authentication {   ~~~ 중략 ~~~ root&gt; show configuration interfaces &lt;인터페이스명&gt; unit 0 {   family inet {     filter {       input icmp;     }   }   address 10.10.0.1/24; } </pre> |





| CISCO    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치<br>방법 | <pre> alerts          Immediate action needed (severity=1) critical         Critical conditions (severity=2) errors           Error conditions (severity=3) warnings         Warning conditions (severity=4) notifications    Normal but significant conditions(severity=5) informational    Informational messages (severity=6) debugging        Debugging messages (severity=7)  Router(config)#exit Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]  Router#show log Syslog logging: enabled (11 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)   Console logging: level debugging, 18 messages logged, xml disabled,   filtering disabled   Monitor logging: level debugging, 0 messages logged, xml disabled,   filtering disabled   Buffer logging: level informational, 1 messages logged, xml disabled,   filtering disabled   Logging Exception size (4096 bytes)   Count and timestamp logging messages: disabled   Trap logging: level informational, 22 message lines logged --More-- *Mar  1 00:01:05.283: %SYS-5-CONFIG_I: Configured from console by console Log Buffer (8092 bytes): </pre> |
| Juniper  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 점검<br>방법 | <p>■ 로깅 파일 확인(설정 및 정상 로깅 여부 확인)</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력] --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@RE:0% cli root&gt; show configuration system syslog user * {     any emergency; } file messages {     any notice;     authorization info; } file interactive-commands {     interactive-commands any; } root&gt; show log total 3704 -rw-rw---- 1 root  wheel  16297 Dec  2 22:38 interactive-commands -rw-rw---- 1 root  wheel   9260 Dec  2 06:30 interactive-commands.0.gz -rw-rw---- 1 root  wheel  11619 Jan 20 2016 interactive-commands.1.gz -rw-r----- 1 root  wheel 599294 Dec  2 06:30 chassisd -rw-r--r-- 1 root  wheel 131922 Jan 20 2016 cosd -rw-r----- 1 root  wheel 468781 Dec  2 06:30 dcd -rw-rw---- 1 root  wheel     0 Dec  2 06:21 default-log-messages -rw-r----- 1 root  wheel 123772 Dec  2 22:38 dhcp_logfile -rw-r----- 1 root  wheel  4660 Dec  2 22:29 dhcp_logfile.0.gz -rw-r----- 1 root  wheel  4868 Dec  2 22:20 dhcp_logfile.1.gz </pre>                                                                                                                                                                                                     |

## Juniper

### ■ Juniper 로깅 관련 참고 사항

- Junos OS 시스템 로그 기본 최대 크기는 플랫폼 유형에 따라 다름
  - EX 시리즈 스위치의 경우 128킬로바이트(KB)
  - M Series, MX 시리즈 및 T 시리즈 라우터의 경우 1메가바이트(MB)
  - TX Matrix 또는 TX Matrix Plus 라우터의 경우 10MB
  - QFX 시리즈 1MB
- logfile 활성 로그 파일이 최대 크기에 도달하면 로깅 유틸리티는 새로운 logfile 파일에 기록하는 파일 로테이션을 수행하며, 최대 10개의 아카이브 파일을 생성
  - 최대 아카이브 파일 수에 도달 하거나, 파일이 설정한 최대 크기에 도달하면 오래된 로그 파일부터 순차적으로 덮어쓰

### [참고] Specifying Log File Size, Number, and Archiving Properties, Juniper Networks

<https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/system-logging-on-a-single-chassis-system.html#id-specifying-log-file-size-number-and-archiving-properties>

### ■ Juniper 로깅 설정 변경

조치  
방법

```
Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@RE:0% cli
root> configure
Entering configuration mode
root# set system syslog archive files 20 ## 예) 아카이브 파일 수 20개 변경
root# set system syslog archive size 2000000 ## 예) 아카이브 파일 크기 2MB로 변경

새로운 로그파일 생성 set system syslog file [파일명] [로그종류] [로그등급]
root# set system syslog file kisalogtest any any
root# commit
commit complete

root# show system syslog
archive size 2000000 files 20;
user * {
 any emergency;
}
file messages {
 any notice;
 authorization info;
}
file interactive-commands {
 interactive-commands any;
}
file kisalogtest {
 any any;
}
```

| 기능관리                                                                                                | 12. 미사용 인터페이스 비활성화                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----------|-----------------------|----------|--------|--------|----------|-----------------|------------|-----|-------|----|----|-----------------|-------------|-----|-------|----|----|-------------------|------------|-----|-------|----|------|-------------------|------------|-----|-------|----|------|-------------|------------|-----|-------|-----------------------|------|-------------|------------|-----|-------|-----------------------|------|-------|------------|-----|-------|-----------------------|
| 보안 위협                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 불필요한 외부 접속 포트 및 인터페이스를 통해 비인가자가 장비 콘솔 또는 네트워크에 무단으로 접속할 수 있는 위험이 존재하므로, 사용하지 않는 포트 및 인터페이스를 비활성화 필요 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 판단 기준                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 양호                                                                                                  | 불필요한 포트 및 인터페이스 사용을 제한하고 있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 취약                                                                                                  | 불필요한 포트 및 인터페이스 사용을 제한하지 않은 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| CISCO                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 점검<br>방법                                                                                            | ■ 사용 중인 포트 및 인터페이스 확인                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
|                                                                                                     | <div>User Access Verification<br/>Password:[패스워드 입력]<br/>Router&gt;enable<br/>Password:[패스워드 입력]<br/>Router#show running-config<br/>show running-config<br/>Building configuration...<br/>Current configuration : 1859 bytes<br/>!<br/>line aux 0<br/>exec-timeout 5 0<br/>!<br/>Router# show ip interface brief<br/>## line 활성화 정보 확인<br/><table><thead><tr><th>Interface</th><th>IP-Address</th><th>OK?</th><th>Method</th><th>Status</th><th>Protocol</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>10.10.10.2</td><td>YES</td><td>NVRAM</td><td>up</td><td>up</td></tr><tr><td>FastEthernet0/1</td><td>192.168.1.1</td><td>YES</td><td>NVRAM</td><td>up</td><td>up</td></tr><tr><td>FastEthernet0/0/0</td><td>unassigned</td><td>YES</td><td>unset</td><td>up</td><td>down</td></tr><tr><td>FastEthernet0/0/1</td><td>unassigned</td><td>YES</td><td>unset</td><td>up</td><td>down</td></tr><tr><td>Serial0/1/0</td><td>unassigned</td><td>YES</td><td>NVRAM</td><td>administratively down</td><td>down</td></tr><tr><td>Serial0/1/1</td><td>unassigned</td><td>YES</td><td>NVRAM</td><td>administratively down</td><td>down</td></tr><tr><td>Vlan1</td><td>unassigned</td><td>YES</td><td>NVRAM</td><td>administratively down</td><td>down</td></tr></tbody></table><br/>## interface 활성화 정보 확인</div> |     | Interface | IP-Address            | OK?      | Method | Status | Protocol | FastEthernet0/0 | 10.10.10.2 | YES | NVRAM | up | up | FastEthernet0/1 | 192.168.1.1 | YES | NVRAM | up | up | FastEthernet0/0/0 | unassigned | YES | unset | up | down | FastEthernet0/0/1 | unassigned | YES | unset | up | down | Serial0/1/0 | unassigned | YES | NVRAM | administratively down | down | Serial0/1/1 | unassigned | YES | NVRAM | administratively down | down | Vlan1 | unassigned | YES | NVRAM | administratively down |
| Interface                                                                                           | IP-Address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | OK? | Method    | Status                | Protocol |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| FastEthernet0/0                                                                                     | 10.10.10.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | NVRAM     | up                    | up       |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| FastEthernet0/1                                                                                     | 192.168.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | YES | NVRAM     | up                    | up       |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| FastEthernet0/0/0                                                                                   | unassigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | unset     | up                    | down     |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| FastEthernet0/0/1                                                                                   | unassigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | unset     | up                    | down     |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| Serial0/1/0                                                                                         | unassigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | NVRAM     | administratively down | down     |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| Serial0/1/1                                                                                         | unassigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | NVRAM     | administratively down | down     |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| Vlan1                                                                                               | unassigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | YES | NVRAM     | administratively down | down     |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
| 조치<br>방법                                                                                            | ■ 미사용 포트 및 인터페이스 사용 제한 및 비활성화                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |
|                                                                                                     | <div>User Access Verification<br/>Password:[패스워드 입력]<br/>Router&gt;enable<br/>Password:[패스워드 입력]<br/>Router# configure terminal<br/>Router(config)#line aux 0<br/>Router(config-line)#exec-time 0 1<br/>Router(config-line)#no exec<br/>Router(config-line)#no login<br/>Router(config-line)#exit<br/>Router(config)# interface fastethernet 0/0/0<br/>Router(config-if)# shutdown<br/>Router(config)# exit<br/>## AUX 사용제한<br/><br/>## interface 비활성화</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |     |           |                       |          |        |        |          |                 |            |     |       |    |    |                 |             |     |       |    |    |                   |            |     |       |    |      |                   |            |     |       |    |      |             |            |     |       |                       |      |             |            |     |       |                       |      |       |            |     |       |                       |



| CISCO    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치<br>방법 | <pre> Router#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]  Router#show running-config                                     ## AUX 설정 확인 Building configuration... Current configuration : 1859 bytes ~~~중략~~~ line aux 0 exec-timeout 0 1 no exec no login ! ~~~중략~~~ Router# show ip interface brief                               ## interface 활성화 정보 확인  Interface      IP-Address OK? Method Status      Protocol FastEthernet0/0 10.10.10.2 YES NVRAM  up          up FastEthernet0/1 192.168.1.1 YES NVRAM  up          up FastEthernet0/0/0 unassigned YES unset  administratively down down FastEthernet0/0/1 unassigned YES unset  up          down Serial0/1/0      unassigned YES NVRAM  administratively down down Serial0/1/1      unassigned YES NVRAM  administratively down down Vlan1            unassigned YES NVRAM  administratively down down </pre> |
| Juniper  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 점검<br>방법 | <p>■ 사용 중인 포트 및 인터페이스 확인</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력]  --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@RE:0% cli root&gt; configure Entering configuration mode root# show system ports {     auxiliary disable; } root#exit root&gt; show interfaces terse  Interface      Admin Link Proto  Local          Remote ge-0/0/0       up    up    inet   192.168.0.100/24 ge-0/0/0.0     up    up    inet   192.168.0.100/24 ge-0/0/1       up    down ge-0/0/1.0     up    down  inet   10.10.0.1/24 ge-0/0/2       up    down ge-0/0/2.0     up    down  eth-switch ge-0/0/3       up    down ge-0/0/3.0     up    down  eth-switch </pre>                                                                                                                                                                                                                                                      |

## Juniper

## ■ 미사용 포트 및 인터페이스 사용 제한 및 비활성화

조치  
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@:RE:0% cli
root> configure
Entering configuration mode
root# set system ports auxiliary disable ## Auxiliary 비활성화
root# set interfaces ge-0/0/1.0 disable ## 미사용 인터페이스 비활성화
root# set interfaces ge-0/0/1.1 disable
root# commit
commit complete

root# exit
root> show interfaces terse

```

| Interface  | Admin | Link | Proto      | Local            | Remote |
|------------|-------|------|------------|------------------|--------|
| ge-0/0/0   | up    | up   |            |                  |        |
| ge-0/0/0.0 | up    | up   | inet       | 192.168.0.100/24 |        |
| ge-0/0/1   | down  | down |            |                  |        |
| ge-0/0/1.0 | down  | down | inet       | 10.10.0.1/24     |        |
| ge-0/0/2   | up    | down |            |                  |        |
| ge-0/0/2.0 | up    | down | eth-switch |                  |        |
| ge-0/0/3   | up    | down |            |                  |        |
| ge-0/0/3.0 | up    | down | eth-switch |                  |        |
| ge-0/0/4   | up    | down |            |                  |        |
| ge-0/0/4.0 | up    | down | eth-switch |                  |        |

| 기능관리                                                                                                                                                                | 13. 불필요한 서비스 비활성화                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 보안 위협                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>사용하지 않는 불필요한 서비스가 활성화된 경우 비인가자가 불필요 서비스의 취약점을 악용하여 공격을 시도 할 수 있으므로, 잠재적 위협으로부터 보호하기 위해 미사용, 불필요 서비스 비활성화</p> <p>* 불필요한 서비스 예) SNMP, WebUI, pad 등(사용 여부검토 필요)</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 판단 기준                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 양호                                                                                                                                                                  | 미사용, 불필요한 서비스가 존재하지 않는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 취약                                                                                                                                                                  | 미사용, 불필요한 서비스가 활성화 되어있는 경우                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CISCO                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 점검<br>방법                                                                                                                                                            | <p>■ 설정 정보 확인을 통해 불필요한 서비스 활성화 여부 확인</p> <p>- HTTP Server, pad, SNMP 서비스 확인 예</p> <pre> User Access Verification Password:[패스워드 입력] Router&gt;enable Password:[패스워드 입력] Router# show ip http server all                                ## http server 실행 확인 HTTP server status: Enabled HTTP server port: 80 HTTP server authentication method: enable HTTP server access class: 0 HTTP server base path: Maximum number of concurrent server connections allowed: 5 ~~~중략~~~ Router# show running-config                                    ## no service pad 확인 Building configuration... Current configuration : 1093 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! Router# show snmp                                             ## snmp 실행 확인 Chassis: FF1045C5 0 SNMP packets input   0 Bad SNMP version errors   0 Unknown community name   0 Illegal operation for community name supplied   0 Encoding errors   0 Number of requested variables   0 Number of altered variables   0 Get-request PDUs   0 Get-next PDUs   0 Set-request PDUs   0 Input queue packet drops (Maximum queue size 1000) 0 SNMP packets output </pre> |

| CISCO    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 조치<br>방법 | <p>■ 설정을 통해 불필요, 미사용 서비스 비활성화</p> <pre> User Access Verification Password:[패스워드 입력] Router&gt;enable Password:[패스워드 입력] Router#configure terminal Router(config)# no service pad                ## pad 서비스 비활성화 Router(config)# do show running-config Building configuration... Current configuration : 1246 bytes ! version 12.4 no service pad service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! Router(config)# no snmp-server                ## snmp 서비스 비활성화 Router(config)# do show snmp %SNMP agent not enabled  Router(config)#no ip http server              ## http server 비활성화 Router(config)#do show ip http server all HTTP server status: Disabled HTTP server port: 80 </pre> |
|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Juniper  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 점검<br>방법 | <p>■ 설정 정보 확인을 통해 불필요한 서비스 활성화 여부 확인</p> <p>- Web-management, SNMP 서비스 확인 예</p> <pre> Amnesiac (ttyu0) login: root Password: :[패스워드 입력]  --- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC root@RE:0% cli root&gt; configure Entering configuration mode root# show ## Last changed: 2023-12-03 03:13:35 KST version 12.3R12.4; ~~~중략~~~ services {   finger;   ftp;   ssh {     protocol-version v2;   }   web-management {     http {       port 80;     }   }   snmp {     community kisatest;   } } </pre> <p>## Web-management서비스 확인</p> <p>## SNMP 서비스 확인</p>                                                                                                                                                                                   |
|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



## Juniper

## ■ 설정을 통해 불필요, 미사용 서비스 비활성화

조치  
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@RE:0% cli
root> configure
Entering configuration mode
root# delete system services web-management ## Web-management 설정 삭제
root# delete snmp ## SNMP 설정 삭제
root# commit
commit complete

root# show ## 설정확인을 통해 정상 삭제 확인
Last changed: 2023-12-03 03:34:27 KST
version 12.3R12.4;
~~~중략~~~
services {
    finger;
    ftp;
    ssh {
        protocol-version v2;
    }
}
~~~중략~~~

```

| 기능관리                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 14. 취약한 서비스 비활성화             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>보안 위협</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                              |
| 취약한 서비스를 공격하여 장비의 장애를 발생시키거나, 연결된 장치에 대한 추가 정보 습득 등 추가 공격에 악용될 수 있어, 취약한 서비스 비활성화 권고<br>* 취약한 서비스 예) Finger, TCP/UDP small, Bootp, CDP, Identd, Domainlookup 등                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                              |
| <b>판단 기준</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                              |
| <b>양호</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 취약한 서비스를 비활성화 및 차단하여 운영하는 경우 |
| <b>취약</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 취약한 서비스가 활성화하여 운영하는 경우       |
| <b>참고 사항</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                              |
| <p>■ <b>Finger :</b></p> <ul style="list-style-type: none"> <li>Finger 서비스는 네트워크를 통하여 연결된 다른 사용자에게 등록된 장치에 대한 정보를 제공하여, 로그인 계정, 접속 IP 등 장비 접속 상태가 노출될 위험성이 존재</li> </ul> <p>■ <b>TCP/UDP small :</b></p> <ul style="list-style-type: none"> <li>진단용으로 설계된 서비스로, DoS 공격 대상이 될 수 있는 서비스인 echo, discard, daytime, chargen을 기본적으로 제공하여 보안상 위협이 존재<br/>※ Cisco IOS 11.2 버전 이하에서는 기본적으로 활성화, 11.3이상 버전에서는 비활성화</li> </ul> <p>■ <b>CDP(Cisco Discovery Protocol) :</b></p> <ul style="list-style-type: none"> <li>Cisco 제품 관리 목적으로 만든 프로토콜로 동일 네트워크에 있는 장비들과 정보를 공유하고, 같은 세그먼트에 있는 다른 라우터에 정보(IOS version, model, device, 연결 정보 등)를 제공</li> </ul> <p>■ <b>Bootp(Bootstrap Protocol) :</b></p> <ul style="list-style-type: none"> <li>네트워크를 이용하여 사용자가 OS를 로드할 수 있게 하고 자동으로 IP주소를 받게 하는 프로토콜로, 다른 라우터의 OS 사본에 접속하여 OS 복사본을 다운로드할 수 있음</li> </ul> <p>■ <b>Source routing :</b></p> <ul style="list-style-type: none"> <li>송신측에서 데이터에 routing 경로를 포함하여 패킷을 routing 시키는 방법으로 공격자가 Source routing 된 패킷을 네트워크 내부로 발송하여 수신된 패킷에 반응하는 메시지를 가로채 공격할 수 있음</li> </ul> <p>■ <b>identd :</b></p> <ul style="list-style-type: none"> <li>특정 TCP연결을 시작한 클라이언트 운영체제와 사용자 ID와 같은 신원을 확인하는 서비스로 비인가자에게 사용자 정보가 노출될 수 있음</li> </ul> <p>■ <b>domain lookup :</b></p> <ul style="list-style-type: none"> <li>CISCO 장비 privileged exec 모드에서 명령어가 아닌 문자열을 입력 시 호스트 이름으로 간주하고 domain lookup을 시도하여 불필요한 DNS 브로드캐스트 트래픽과 사용자 대기시간 발생</li> </ul> |                              |

## CISCO

## ■ 설정 확인을 통해 취약한 서비스 활성화 확인

점검  
방법

```

User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#show running-config
Building configuration...

Current configuration : 1321 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service udp-small-servers ## udp small 서비스
service tcp-small-servers ## tcp small 서비스
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
! ip finger ## finger 서비스
ip tcp synwait-time 5
!
ip identd ## identd 서비스
No cdp log mismatch duplex
Cdp timer 50
!
Router# show cdp ## CDP서비스
Global CDP information:
 Sending CDP packets every 50 seconds
 Sending a holdtime value of 180 seconds
 Sending CDPv2 advertisements is enabled

```

## CISCO

## ■ 설정을 통해 취약한 서비스 비활성화

조치  
방법

```

User Access Verification
Password:[패스워드 입력]
Router>enable
Password:[패스워드 입력]
Router#configure terminal
Router#no ip finger ## finger서비스 차단
Router#no service udp-small-servers ## udp small 서비스 차단
Router#no service tcp-small-servers ## tcp small 서비스 차단
Router#no cdp run ## CDP서비스 차단
Router#no ip bootp server ## bootp 서비스 차단
Router#no ip source-route ## source route 서비스 차단
Router#no ip identd ## identd 서비스 차단
Router#no ip domain-lookup ## domain-lookup 서비스 차단
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Router#show running-config
Building configuration...
Current configuration : 1268 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
boot-start-marker
boot-end-marker
!
no ip source-route
no ip icmp rate-limit unreachable
!
no ip domain lookup
!
!
!
no cdp log mismatch duplex
no cdp run

```

## Juniper

## ■ 설정 확인을 통해 취약한 서비스 활성화 확인

점검  
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@:RE:0% cli
root> configure
Entering configuration mode
root# show
Last changed: 2023-12-03 05:37:49 KST
version 12.3R12.4;
system {
 time-zone Asia/Seoul;
 no-redirects;
 ports {
 auxiliary disable;
 }
 services {
 finger { ## finger 서비스 확인
 connection-limit 5;
 }
 ssh {
 protocol-version v2;
 }
 tftp-server { ## tftp 서비스 확인
 connection-limit 5;
 }
 dhcp {
 traceoptions {
 file dhcp_logfile;
 level all;
 flag all;
 }
 }
 }
}

forwarding-options { ## bootp 서비스 확인
 helpers {
 bootp {
 server 192.168.0.20;
 }
 }
}

routing-options { ## source-routing 서비스 확인
 source-routing {
 ip;
 }
}

```

## Juniper

## ■ 설정을 통해 취약한 서비스 비활성화

조치  
방법

```

Amnesiac (ttyu0)
login: root
Password: :[패스워드 입력]

--- JUNOS 12.3R12.5 built 2016-01-20 04:27:51 UTC
root@RE:0% cli
root> configure
Entering configuration mode
[edit]
root# delete system services tftp-server ## tftp 서비스 차단
[edit]
Root# delete system services finger ## finger 서비스 차단
[edit]
Root# delete forwarding-options helpers bootp ## bootp 서비스 차단
[edit]
Root# delete routing-options source-routing ## source-routing 서비스 차단
[edit]
root# commit
commit complete
[edit]
root# show ## 설정확인을 통해 정상 삭제 확인
Last changed: 2023-12-03 05:54:22 KST
version 12.3R12.4;
system {
 time-zone Asia/Seoul;
 no-redirects;
 ports {
 auxiliary disable;
 }
 root-authentication {
 encrypted-password "1QMC0$CLj7QGouafegdNNoisdaF6dwkim/";
 }
 login {
 class timeout {
 idle-timeout 5;
 }
 }
 services {
 ssh {
 protocol-version v2;
 }
 dhcp {
 traceoptions {
 file dhcp_logfile;
 level all;
 flag all;
 }
 }
 }
}

```



# 중소기업 네트워크 장비 보안점검 안내서



**발행일** 2024년 1월

**집필** 한국인터넷진흥원 침해예방단 기업보안점검팀  
김대완 선임, 조세준 선임  
배승권 팀장

**감수** 최광희 본부장, 임진수 단장

본 보고서의 내용에 대해 진흥원의 허가 없이 무단전재 및 복사를 금하며,  
위반 시 저작권법에 저촉될 수 있습니다.