

# XTM VPN

## CHECK LIST

순차적인 Check 과정.

1. 장비 외관 상태확인
2. 네트워크 장비 체크 (ifconfig, ping, route, iptables -L)
3. VPN 상태 체크 (sainfo tunnel, capture , show traffic 0....)
4. 장비 백업 방법

### 1. 장비 외관 상태 확인

LED 링크 상태, 케이블 연결 상태, 후면 팬동작 상태, 전체적인 외관 상태 확인

### 2. 네트워크 장비 체크

# ifconfig

```
# ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:15:78:34
      inet addr: 10.0.0.1 Bcast: 10.0.0.255 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:327157834 errors:0 dropped:0 overruns:0 frame:0
      TX packets:426028761 errors:0 dropped:4007 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:173583538268 (161.6 GiB)  TX bytes:485953529286 (452.5 GiB)

eth1:  Link encap:Ethernet HWaddr 08:00:27:15:78:35
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

인터페이스 설정 상태 확인

## # ping

```
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=52 time=29.7 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=29.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=29.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=29.5 ms
```

네트워크 통신 상태 확인 (내/외부 상태 체크)

## # route

```
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 255.255.255.224 U 0 0 0 eth2
192.168.1.0 192.168.1.1 255.255.255.0 UG 1 0 0 eth0
192.168.1.1 192.168.1.1 255.255.255.0 U 0 0 0 eth0
192.168.1.1 192.168.1.1 0.0.0.0 UG 1 0 0 eth2
```

라우팅 등록 상태 확인 (이전 상태와 비교)

※ GUI 접속 – 설정 – 네트워크 - 라우팅에서도 확인가능

## # iptables -L

```
# iptables -L
Guardian SPD manager (policy DROP)
Chain INPUT (policy DROP)
0 0 0 0 0 0 ACCEPT 0 -- 0.0.0.0/0 0.0.0.0/0
0 0 0 0 0 0 ACCEPT 0 -- 127.0.0.1 127.0.0.1
2 62 2 0 56 0 0 IPSEC 0 -- 0.0.0.0/0 0.0.0.0/0
5 1 5 0 56 0 0 DROP 0 -- 192.168.1.1 192.168.1.1
8 2 8 0 56 0 0 DROP 0 -- 192.168.1.1 192.168.1.1
9 5 9 680 56 0 0 ACCEPT 0 -- 0.0.0.0/0 0.0.0.0/0
10 4 10 680 56 0 0 ACCEPT 0 -- 0.0.0.0/0 0.0.0.0/0
13 17 13 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
14 8 14 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
15 16 15 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
16 15 16 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
17 17 17 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
18 59 18 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
19 0 0 0 56 680 19 67 IPSEC 0 -- 0.0.0.0/0 0.0.0.0/0
Chain OUTPUT (policy DROP)
20 18 20 680 62 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
21 60 21 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
22 68 22 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
23 69 23 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
24 61 24 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
25 64 25 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
26 58 26 680 56 0 0 IPSEC 0 -- 192.168.1.1 192.168.1.1
29 54 29 680 56 0 0 ACCEPT 0 -- 192.168.1.1 192.168.1.1
30 55 30 680 56 0 0 ACCEPT 0 -- 192.168.1.1 192.168.1.1
31 56 31 680 56 0 0 ACCEPT 0 -- 192.168.1.1 192.168.1.1
32 11 32 680 56 0 0 ACCEPT 0 -- 192.168.1.1 192.168.1.1
```

방화벽 정책 등록 상태 확인 (이전 상태와 비교)

※ GUI 접속 – 설정 – 필터링 – ipv4 필터링 에서도 확인가능

※ 그 외 설정에 대해서도 사전체크가 필요

## # cat /var/log/messages

```
# cat /var/log/messages
Apr 11 11:46:40 Future syslog.info syslogd started: BusyBox v1.4.1
Apr 11 11:46:40 Future user.notice kernel: klogd started: BusyBox v1.4.1 (2017-08-31 12:22:22 KST)
Apr 11 11:46:40 Future user.notice kernel: WeGuardia XTM XOS version 2.6.20, #1 SMP Tue May 15 10:39:52 KST 2018
Apr 11 11:46:40 Future user.warn kernel: CVMSEG size: 2 cache lines (256 bytes)
Apr 11 11:46:40 Future user.warn kernel: CPU revision is: 000d0708
Apr 11 11:46:40 Future user.warn kernel: Determined physical RAM map:
Apr 11 11:46:40 Future user.warn kernel: memory: 0000000010000000 @ 0000000000000000 (usable)
Apr 11 11:46:40 Future user.warn kernel: memory: 0000000070000000 @ 0000000041000000 (usable)
```

시스템 로그 확인

## # dmesg

```
# dmesg
of class 10010 is small. Consider r2q change.
kjournald starting. Commit interval 5 seconds
EXT3 FS on cfa2, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
New_Master_Obj File Name None
Info: Load extended script len[25]...
ok
[20200413-10:43:44]: Complete to apply policy object
Finished reinitializing the system config.
Configuration mode start [Console]
Cache error exception:
```

커널 시스템 로그 확인

## 3. VPN 상태 체크

### # admin

명령어를 통해 Admin 모드로 전환

### admin# sainfo tunnel

터널 상태 정보를 확인하는 명령어 입니다. TED 상태와 IKE 상태, DPD 확인 해야 합니다.

IKE 상태에 finished 떴야 터널이 연결 된 것입니다. Finished 가 안 뜨고 progress 가 뜨는 것은

ISAKMP SA 설정 값이 서로 다를 경우 발생합니다.

Sainfo 명령어에는 tunnel 외에 -index 번호를 적어 부분적으로 확인 하는 방법이 있습니다.

그 외 sa1, sa2 옵션들을 가지고 있으며, -s 옵션을 통해 터널 맺어진 개수 확인이 가능합니다.

```
admin# sainfo -s
*** Table Status ***
*** IPSEC ***
TED : count[ 2 / 4001] size[ 368 x 4001 = 1472368]
KT : count[ 0 / 1] size[ 1804 x 1 = 1804]
SA1 : count[ 2 / 4001] size[ 104 x 4001 = 416104]
SA2 : count[ 2 / 4001] size[ 620(228) x 4001 = 2480620]
```

현재 2개 터널 연동된 상태 확인 가능. (다수 터널을 붙였을 때 유용하게 사용되는 명령어)  
 상황에 따라서 실제 터널 수보다 많게 찍히는 경우가 발생 (실제 터널 맺어지지 않는 경우,  
 응답 요청에 따라 카운터 수가 증가하여, 시간이 지남에 따라 원래대로 정상수치로 돌아옴)

## admin# capture [ IP ]

IP 대한 서비스 상태 체크

## admin# capture [ icmp | esp ] 또는 포트

500번 포트에 대한 캡처를 하면 ESP, IKE 정보를 주고 받는지 확인 할 수 있습니다.

실제로 서비스 되고 있는지 확인 하기 위해서는 Capture [대상 서버 IP] 로 체크 가능합니다.

서버 IP 가 많아 확인이 힘들 때는 ex) Capture 192.168.0. <- 이런 식으로 마지막을 점으로 하여 그 밑에 해당하는 네트워크 영역을 체크 가능합니다.

또한 Capture [interface]를 통해 인터페이스에 대한 통신 체크를 확인 할 수 있습니다.

캡처에 대해 더 자세한 정보 출력을 원한다면 admin#sv a 1 명령어를 통해

추가적으로 확인 할 수 있는 부분(암/복호화 상태, 패킷 적용 룰)이 많아 집니다.

캡처 내용간 EN은 암호화, DE는 복호화 인 것을 확인 가능

Ex) Capture 500 (enter)

Capture 1.1.1.1 (enter)

캡처를 다 하였으면, Ctrl + C 또는 Capture 0 을 통해 캡처 종료 시킬 수 있습니다.

Sv a 1 명령어를 사용하여 캡처하고 캡처가 마무리 되면, Sv a 0 을 통해 옵션을 끕니다.

## admin# show traffic 0

```
admin# show traffic 0
```

		eth0	eth1	eth2	eth3	eth4	eth5	eth6	
BITS (bps)	RX	2.97 K	0	5.96 K	0	0	0	0	
	TX	3.88 K	0	1.04 K	0	0	0	0	
COUNT (pps)	RX	3	0	8	0	0	0	0	
	TX	5	0	1	0	0	0	0	
INFO [CPU:4%, MEM:36%, SESS:57, CPS:0 LOG:3958197, TUNNEL:2, IKE(SA:0/0,TED:0/7,DPD:228928,RX:342260)]									

장비 실시간 트래픽 확인

## admin# ted show

Ted 테이블에 대한 정보 값을 출력하기 위해 사용 되는 명령어.

터널이 맺어지면 상대방에 CID와 보안호스트 값을 확인 할 수 있습니다.

그 외 확인할 부분은 alloc\_tm 과 update\_tm 부분입니다.

Alloc\_tm : 터널이 할당 된 시간.

Update\_tm : 터널이 갱신 된 시간.

정책 전송을 하게 되면 두 개의 시간이 전부 초기화 됩니다.

```
alloc_tm [2017.09.07 10:43:41]
update_tm [2017.09.07 10:43:43]
```

상대방에서 정책 전송을 했을 시에는 본 장비에서는 update\_tm만 변경이 됩니다.

```
alloc_tm [2017.09.07 10:43:41]
update tm [2017.09.07 10:48:22]
```

## 추가 옵션

ted show -i [WORD] : IPSec VPN 사용 시, ted 테이블에서 특정 인덱스에 대한 정보를 출력합니다.

ted show -ip [A.B.C.D] : IPSec VPN 사용 시, ted 테이블서 특정 IP 주소에 대한 ted 정보를 출력합니다.

**admin# trap\_buf -r**

펌웨어 정보 확인

**admin# status d**

```
admin# status d*** Link Information
*** Ethernet Interface 0, 1, ... Infomation
port number      :      0      1      2      3      4      5      6
links status     :      on     off     on     off     off     off     off
links speed      :     1000     0     100     0      0      0      0
links duplex     :       1      0      1      0      0      0      0
```

포트 링크 상태 체크

**[이중화 장비 인 경우 확인]**

**admin# show ad**

장비 이중화 HA 상태 및 세션 동기화 확인

**admin# show ch**

장비 이중화 체커 상태 확인

**[터널이 정상적으로 안 붙는 경우 확인]**

**admin# debug spi**

S : 시스템, P : packet filtering, I : ipsec(detail)

사용하고 정지하려면 Debug s 만 쓰면 됩니다.

이중화 된 장비에 접속하거나 여러 장비에 터널 붙을 때는 CID 값을 IPSec 대상 설정에 입력해야 합니다. 간혹 서로에 CID 값이 달라 접속이 안 되는 경우가 있는데 그때 서로 주고받는 터널 협상 정보를 확인할 수 있는 명령어입니다.

<b>백업</b>		<b>즉시실행</b>
* 비밀번호	<input type="text"/>	* 비밀번호 확인 <input type="password"/>
* 실행주기	<input type="checkbox"/> day <input type="button" value="v"/>	<input type="button" value="v"/>
* 백업은 해당 일 오전 2시에 실행되며 백업데이터는 최대 7개까지 보관됩니다.		
* (S)FTP 백업	<input type="checkbox"/> * [관리기능>로그>로그백업용 (S)FTP서버 설정]이 필요합니다.	
		확인 취소

  

* 설정 복원/초기파일 주입	<input type="text"/>	찾아보기...
* 비밀번호	<input type="text"/>	
		확인 취소

  

### 서비스

☐ 서비스 중단  
☐ 서비스 재개  
☐ 시스템 종료  
☒ 시스템 재시작

☒ 즉시 재시작

---

☐ 예약 재시작

- \* 날짜입력
- \* 시간/분

확인

  

<b>무결성 검사</b>	<b>즉시실행</b>
* 실행주기	<input type="checkbox"/> day <input type="button" value="v"/>

확인