XTM VPN

CHECK LIST

순차적인 Check 과정.

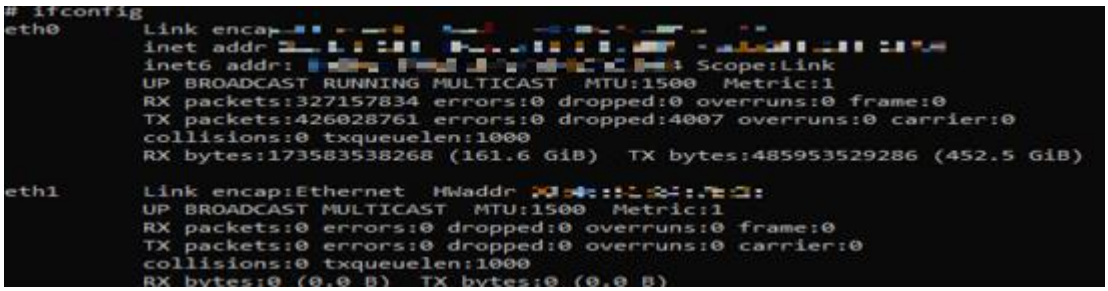
1. 장비 외관 상태확인
2. 네트워크 장비 체크 (ifconfig, ping, route, iptables -L)
3. VPN 상태 체크 (sainfo tunnel, capture , show traffic 0....)
4. 장비 백업 방법

1. 장비 외관 상태 확인

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

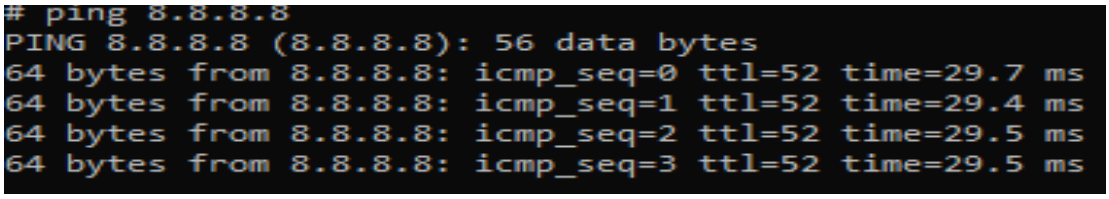
2. 네트워크 장비 체크

ifconfig



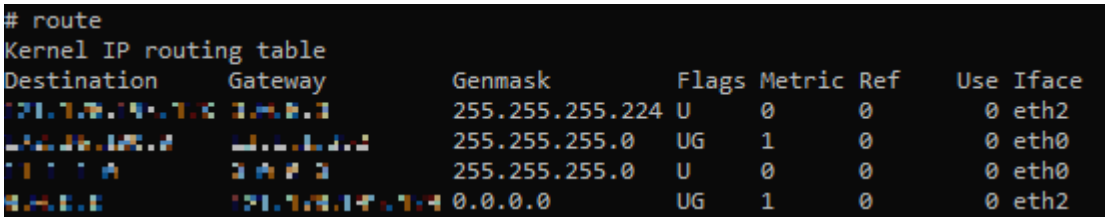
인터페이스 설정 상태 확인

ping



네트워크 통신 상태 확인 (내/외부 상태 체크)

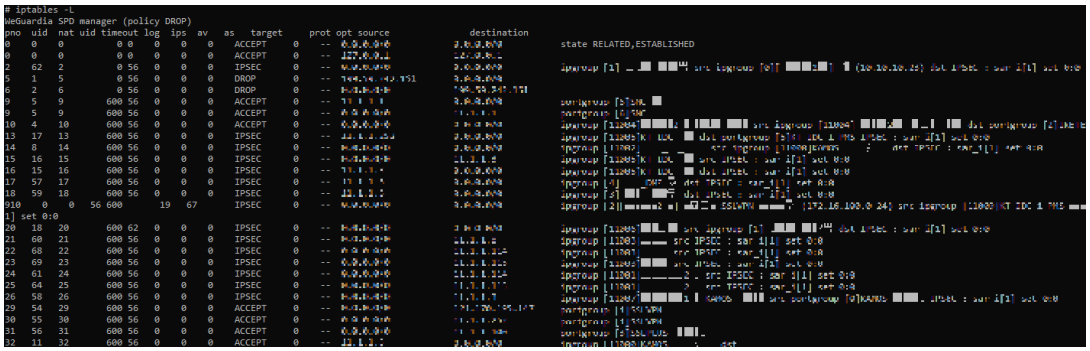
route



라우팅 등록 상태 확인 (이전 상태와 비교)

※ GUI 접속 – 설정 – 네트워크 - 라우팅에서도 확인가능

iptables -L

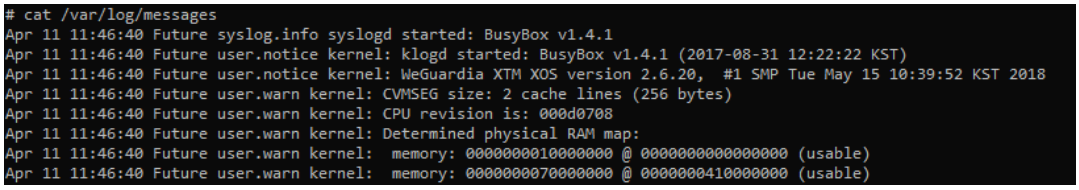


방화벽 정책 등록 상태 확인 (이전 상태와 비교)

※ GUI 접속 – 설정 – 필터링 – Ipv4 필터링 에서도 확인가능

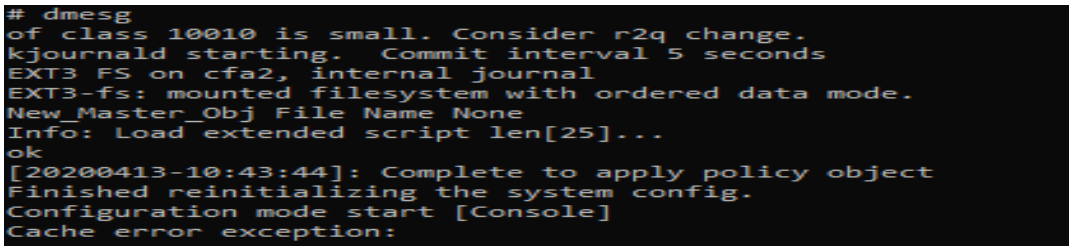
※ 그 외 설정에 대해서도 사전체크가 필요

cat /var/log/messages



시스템 로그 확인

dmesg



커널 시스템 로그 확인

3. VPN 상태 체크

admin

명령어를 통해 Admin 모드로 전환

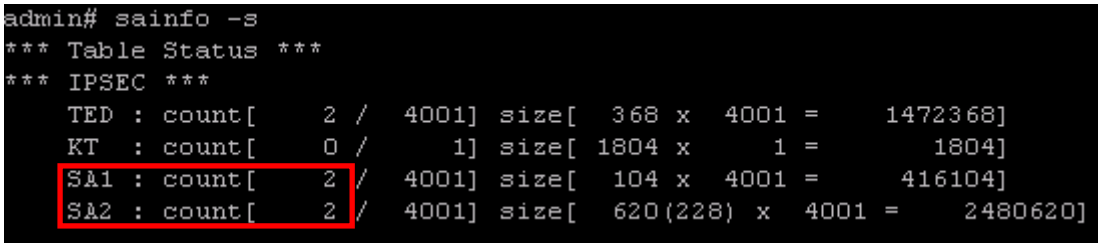
admin# sainfo tunnel

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

IKE 상태에 finished 떠야 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.



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 맺어지지는 않으나,

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 캡쳐를 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

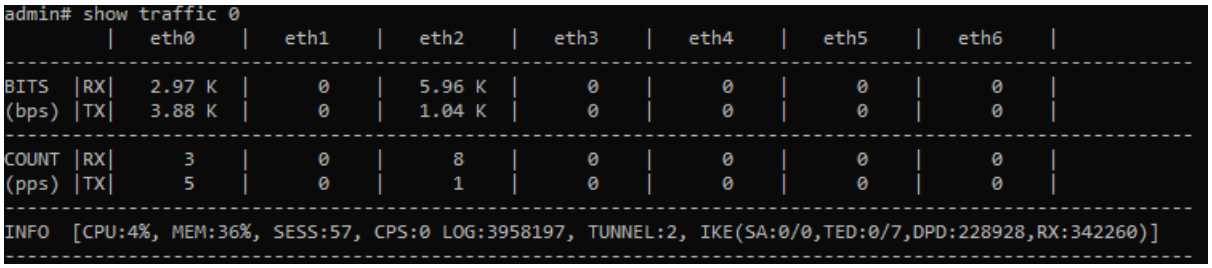
Ex) Capture 500 (enter)

Capture 1.1.1.1 (enter)

캡쳐를 다 하였으면, Ctrl + C 또는 Capture 0 을 통해 캡쳐 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  |RX|   2.97 K  |      0    |   5.96 K  |      0    |      0    |      0    |      0    |
(bps) |TX|   3.88 K  |      0    |   1.04 K  |      0    |      0    |      0    |      0    |
-------------------------------------------------------------------------------------------------
COUNT |RX|      3    |      0    |      8    |      0    |      0    |      0    |      0    |
(pps) |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 인 덱스에 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

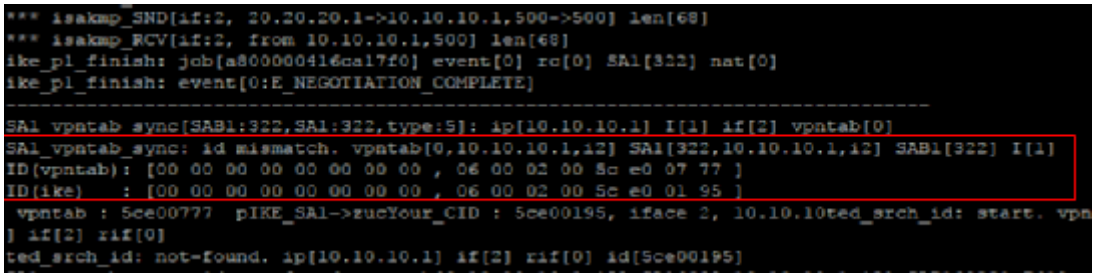
[터널이 정상적으로 안 붙는 경우 확인]

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.



위와 같이 확인 결과 CID 값이 달라 mismatch 되는 것을 확인 가능합니다.

이럴 때는 서로 CID값을 확인하여 맞춰 나가야 합니다.

4. 장비 백업 방법

GUI – 설정 – 시스템 – 시스템 상태 에서 백업 칸 비밀번호 등록 후 즉시실행 버튼을 통해 백업 실시(확장자는 gat로 생성되며 일반 텍스트 뷰어로는 확인 불가능)