2월 25일 SMB Webseminar – Q&A
QoS 솔루션

웹 세미나 시 진행된 질문과 답변 내용 중 중요한 내용을 정리하여
업무에 도움이 되실 수 있도록 전달해 드립니다.

Q1. RDR 말고 EDR (Event Data Record) 도 지원하나요?

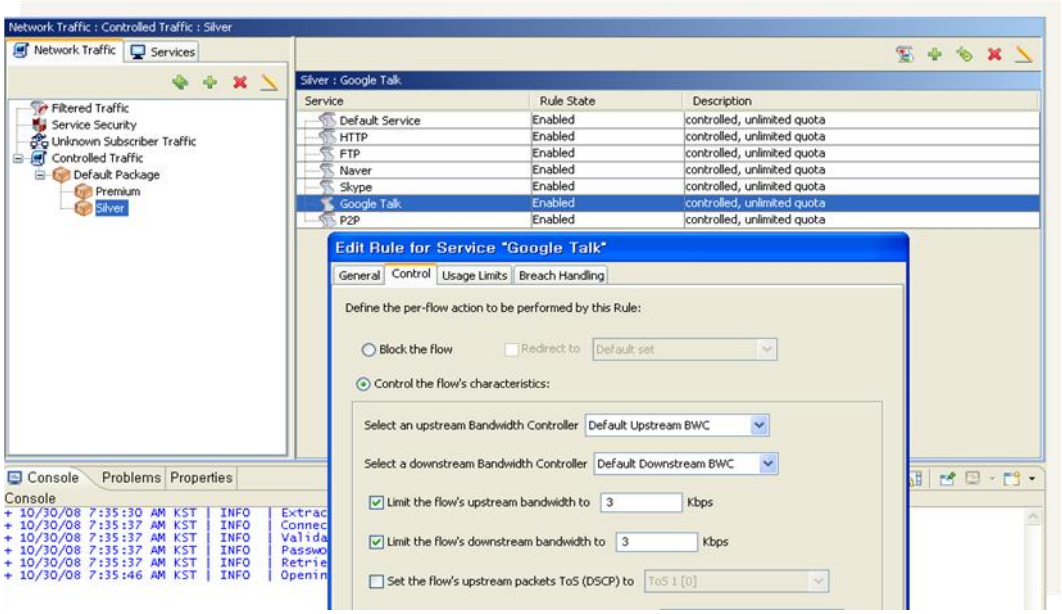
A. EDR이라고 따로 지원하는 포맷은 없습니다. 장비의 장애 정보는 표준 프로토콜인 SNMP Trap 을 통해 일반 NMS를 통해 수신이 가능합니다.

Q2. 현재 피크시간 때 1.5G정도의 트래픽이 흐르고 있는 회선입니다. 이런 경우 SCE2000모델로 커버가 될까요? 아울러 백본이 10G 인터페이스를 이용하고 있는데 SCE2000모델에 10G 인터페이스가 있는지도 궁금합니다.

A. 사용량으로는 SCE2000으로 충분히 처리가 가능합니다. 그런데 SCE2000이 현재는 1G 포트만 지원합니다. 장비에 Giga 포트가 있다면 Hairpin 구성으로 SCE2000을 통과해서 처리하도록 구성할 수도 있습니다. (실제 그렇게 구성하는 사례도 많음).
그게 불가능하다면 SCE8000이 10G를 지원합니다.

Q3. Port or 사이트 정의는 어디에서 하나요?

A. Console 프로그램을 통하면 GUI 기반 설정 화면이 있습니다. 해당 화면을 통해 정책을 만들고 해당 정보를 SCE에 적용하면 그 정책에 맞추어서 SCE가 동작합니다.
* 아래는 Console 정책 설정 화면입니다



Q4. Packet Logic이라는 장비와 차별된 점은?

A. Packet Logic 의 하는 역할과 장비의 목적은 동일합니다. 단, Packet Logic은 가입자 별 관리 기능의 탄력성이나 외부 시스템과의 연동 부분에 다소 블랙박스화 되어있습니다. 그런 유연성 부분이나 시스템 성능 그리고 장비의 가격경쟁력이 우수합니다.

Q5. 모니터링 측면만 고려할 때 NAM과 비교하면 어떠한가요? 기능 및 관리, 비용 측면에서 어떤 것이 더 낫다고 생각하시는지요?

A. 앞에서도 말씀 드렸듯이 NAM은 Application 분석 기준이 L4 기준입니다. SCE는 Behavior 기반이라고 하며, 훨씬 지능도가 높다고 보시면 됩니다. 그리고 SCE는 CM 자체 DB에 데이터가 저장되어 있어서 별도 시스템에서 DB를 통해 원하는 Report를 재생산이 가능한 반면 NAM은 주어진 Report Format을 그대로 활용하거나, CSV로 Export하여 작업을 하나 연동성이 조금 떨어집니다. 고객이 원하는 모니터링의 수준에 따라서 일반적인 Trend 위주라면 NAM이 설치관점이나 사용면에서도 충분하다고 봅니다만 혹시 다이나믹한 Application 분석 및 보고가 필요하거나 Report의 재가공, 보안관련 Report 등을 원하신다면 SCE가 더 적절할 수 있습니다.

Q6. 네트워크가 idc로 통합되어 있지 않고 각 지점별로 구성이 되어있다면 각 지점에 제품이 하나씩 필요한 건가요?

A. 지점과 본사 사이의 트래픽을 제어할 목적이시라면 지점별로 설치하셔야 합니다. 본사를 통해 외부 인터넷 구간을 제어할 목적이시라면 인터넷 인 입구간에 설치하셔야 합니다

Q7. 가격은 어떻게 되나요?

A. SCE1010의 경우 Price List상 USD 30K, SCE2020의 경우 USD 50K 입니다.
Control 용도로 사용할 때는 Control을 위한 라이선스가 10K 있습니다.

Q8. 기존의 QoS와 다른 점은 성능과 패턴인식의 다양화 인가요?

A. 기존의 QoS가 장비 (Router/Switch) 의 QoS라고 한다면 성능과 패턴인식의 다양화입니다.
그리고 실제 QoS를 처리하는 방식이 장비에서는 Queue Handling이라고 한다면 SCE를 통해서는 해당 트래픽 별로 주어진 성향에 대해 훨씬 Detail하게 관리가 된다고 보시면 됩니다.

Q9. Full host, Full connection 정보확인이 되나요?

A. 아래는 RDR의 Sample입니다. 아래와 같은 내용이 Record로 남습니다.
Access_string이 Hostname이며 info_string 부분이 나머지 URL 부분입니다. 참고하십시오.

Transaction RDR(HTTP browsing)	
subscriber_id	1083836365
package_id	9
service_id	16
protocol_id	2
skipped_sessions	1
server_ip	3740262096
server_port	80
access_string	img.empas.com
info_string	/search/common/icon/no_p10.gif
client_ip	1080584418
client_port	43247
initiating_side	0
report_time	1225355289
millisec_duration	10
time_frame	0
session_upstream_volun	662
session_downstream_vo	408
subscriber_counter_id	2
global_counter_id	2
package_counter_id	9
ip_protocol	6
protocol_signature	50397184
zone_id	0
Flavor-id	0
flow_close_mode	0

Q10. DPI장비가 패킷을 검사하는 것으로 인한 추가적인 트래픽은 전혀 없는 건가요?

A. 추가적인 트래픽은 전혀 발생하지 않습니다. DPI 처리하는 성능 자체도 정책 수, 감지하는 Application의 수에 따라서 경쟁사마다 성능차이가 많이 납니다. 시스코의 가장 강점이 바로 해당 처리 성능입니다. 처리 latency가 마이크로 Sec. 단위입니다.

Q11. content filter 할 수 있는 기능이 있다고 하셨는데 차단 기반이 URL 기반이신지?

A. 네. URL 기반입니다.

Q12. 국산 p2p에 대해서 정책 설정이 가능한가요? 현재 지원되고 있는 프로토콜들도 가능한가요?

A. P2p Behavioral이라고 정의되어있는 패턴이 있어서 해당 패턴으로 분석되는 경우도 있습니다. 따로 특정 P2P를 제어하고자 하는데 기존 Protocol Package에 포함되어있지 않을 경우에는 추가 요청 과정을 통해 개발 후 적용이 가능합니다.

Q13. Inside방식에서 사용할 때 internal에 문제가 있을 경우 by pass로 동작하나요? 전환되는데 문제는 없나요?

A. 네. 내부 장비의 문제 혹은 Reload시 동작 방식을 설정할 수 있습니다. Bypass/Cutoff 두 가지가 지원되고요. cutoff시에는 해당 링크를 down시킵니다. (보통 절체용으로 설정함)
전환 기준은 내부 문제에 대해서는 Sanity-Check 기능이 자체적으로 돌아가고 몇 가지 요소에 대해서는 상한선을 지정할 수 있습니다.

Q14. 유해 트래픽 차단기능은 있나요? 예를 들어 패턴매칭이나 Port 정책을 통해서 웜이나 바이러스 등을 차단할 수 있는 기능 등이 지원되나요?

A. Attack Filter 기능이 있어서 특정 port의 초당 세션 수를 기준으로 설정하고 차단이 가능합니다. 패턴 매칭 부분은 별도의 Signature를 추가하면 가능하도록 되어있으나 공식적으로 SCE와 함께 제공되는 Protocol에 해당 signature는 포함되어 있지 않습니다. Signature Editor를 통해서 패턴 정의를 임의로 업데이트할 수 있습니다.

감사합니다