<주요 Q&A>

H/W기반 데이터 가속 카드를 이용한 고속 패킷 처리

Q1. 패킷을 고속처리하면 중간에 패킷을 인터셉트 하는 가능성도 낮아지는 것인지요?

패킷을 모니터링 하는 시스템도 같이 성능이 올라가고 있어 가능성이 낮아진다고 볼수는 없습니다. 다만 봐야할 정도가 더 많아지게 됩니다.

Q2. 기업이 네트워크 보안을 하는 데 있어서 방화벽을 효율적으로 활용할 수 있는 방법에 대해서 질문 드립니다.

기존에는 단순히 네트워크 정보 기반의 접근제어를 수행한데 반해, 최근의 차세대 방화벽은 사용자 정보와 앱인지 정보를 기반으로 좀더 정밀하게 처리할 수 있어 정책 수립이 좀더 친화적으로 바뀌고 있습니다.

Q3. 고속패킷처리를 통해 100G 급 DDoS 탐지 대응도 가능한지 궁금하고 HA 구성등을 해서 극대화 할 수 있는지요

현재까지는 100G급의 대역폭을 처리하기는 하지만, 작은 크기의 패킷에 대한 처리는 여전히 100G 급에 이르지는 못하고 있습니다. HA 구성시는 이를 구성된 장비수만큼 분산하여 처리할 수는 있습니다.

Q4. 네트워크 보안 관련하여 SSL 트래픽을 효율적으로 처리하는 방법에 대해서 문의 드립니다.

보안 부분에 있어서는 사용자의 암호화된 트래픽의 내용에서 위협정보를 찾기 위해 SSL Inspection 이라는 기술을 사용합니다. 그러나 해당 기술은 실시간으로 트래픽의 복호화하여 검사하고 다시 암호화 하는 등의 처리해야할 기능이 많아 성능적인 저하가 큽니다.

Q5. DPU가 무엇인지요? 처음 들어봐요

업체들 마다 이러한 네트워크 카드들의 명칭이 다릅니다.
DPU, IPU, SmartNIC 등의 용어를 사용합니다.

Q6. CPU 기반 자원과 H/W 기반의 고속 패킷 처리 방법을 상호 보완적으로 활용할 수 이는 방안에 대해서 질문 드립니다.

처리해야할 기능에 따라 다르긴 하지만, 본 세션의 예처럼 네트워크 카드에 프로세서들이 포함되면서 기존 대비 다양한 형태의 기능을 처리할 수 있습니다.

Q7. 방화벽을 차세대 기능을 활용한 복합적 방어로 활용할 수 있는 방법에 대해서 문의 드립니다.

차세대 방화벽은 접근제어기능뿐만 아니라 DDoS 방어부터 IPS 기능을 통한 위협 탐지 차단도 지원을 하고 있습니다. 또한 사용자 정보, 앱인지, 디바이스 제어 등의 연동 등을 통해 좀더 복합적인 정책을 수립할 수 있습니다.

Q8. DPU/IPU 를 사용하는 환경은 어떻게 다른지요? 하나로 합쳐서 서비스는 어려운 것인가요?

DPU는 사전 정의된 가속 기능을 칩에 제공하고 있고 IPU는 이를 FPGA를 통해 사용자가 원하는 기능을 만들어 낼 수 있습니다.

Q9. CPU의 부하를 줄여주는 DPU, IPU 성능대비 가격 경쟁력과 안정성이 확보되었는지 궁금합니다.

아직은 업체에서 새롭게 제시하고 있는 솔루션들이기 때문에 기대효과가 큰것도 사실이지만 어느 정도의 경쟁력을 가질 수 있는지에 대해 확인도 필요할 것으로 보입니다.

Q10. DPU는 업계를 선도하는 소프트웨어 정의 네트워킹, 스토리지와 사이버

보안 기능을 데이터센터에 제공하는지 궁금합니다.

발표자료에도 언급되었듯이 데이터센터 적용방안으로 네트워킹, 스토리지, 보안기능이 제공됩니다

Q11. 데이터 처리 장치를 사용하여 차세대 방화벽을 거의 회선 속도로 제공하여 5G 네이티브 보안 솔루션을 구축할 수 있는지 궁금합니다.

아직은 솔루션이 소개된 시점이기에 실제 개발 및 검증을 통해 확인을 해야 할 것으로 보입니다.