<주요 Q&A>

차세대 방화벽을 이용한 안전한 원격근무 환경 구성

Q1. 재택근무 시 방화벽 수정의 경우 참 번거로운 상황이 많더라고요. 테더링/와이파이/자택LAN 등 다양한 환경에서 접속을 관리할 수 있는지 궁금합니다.

자택에서 접속하는 경우에 대해서도 인증서 기반으로 처리 가능합니다. 무선의 경우 SSLVPN 에이전트를 통해 접근 가능합니다. 유/무선 환경 모두 접근할 수 있습니다.

Q2. 원격근무용 장비에서 프로세스 실행 통제가 가능한지 궁금합니다.

방화벽과 연결을 위한 SSLVPN클라이언트에서는 프로세스 통제는 지원하지 않고 있습니다. 다만 필요한 경우 필수 보안 S/W와 연동하여 동작할 수 있습니다.

Q3. 제로트러스트 네트워크를 설명하시면서 말씀하신 요소를 구성할 수 있는 솔루션이 있는지요?

BLUEMAX NGF + CLIENT를 활용하여 설명 드린 내용에 대해 구성 가능합니다.

Q4. 제로트러스트 네트워크는 사용자 엔드포인트 솔루션도 함께 운영 되야 효과가 높은 건지요?

제로트러스트 네트워크의 경우 단말의 보안상태에 대한 확인이 같이 필요합니다. 따라서 같이 운영되어야 효과가 높습니다.

Q5. Client라는 것은 방화벽 클라이언트 프로그램을 이야기하시는 것인지 아니면 다른 솔루션을 이야기하시는 건지 궁금합니다.

기본적으로는 방화벽 Client를 통해 가능하고, 이와 유사한 기능을 지원하는 Client가 별도로 있다면, BLUEMAX NGF의 REST API 연동을 통해 가능할 것 같습니다.

Q6. 어떠한 방법으로 차세대 방화벽에서 사용자 정보를 알 수 있나요?

사용자 정보는 사내에 설치된 AD등 인사정보와 연동하여 자동으로 인지하고 있습니다. 가령 사내에서 AD기반 인증을 사용하신다면 해당 단말에서 AD인증된 내용을 토대로 방화벽에서 이를 인지하는 방식입니다.

Q7. 방화벽에서 어떻게 사용자 보안 환경을 점검하나요?

방화벽 Client 설치가 필요하고, 방화벽 Client에서 단말의 정보를 수집하여 이를 방화벽으로 전송하여 줍니다. 그러면 방화벽에서는 이러한 정보를 기반으로 접근제어 정책을 수립하실 수 있습니다.

Q8. 차세대방화벽에서 암호화된 트래픽에 대한 탐지/차단은 어떤 식으로 가능한지 궁금합니다.

암호화트래픽(SSL)에 대한 복호화 처리 기능이 있어서 방화벽에서 이를 복호화하여 보안처리 후, 다시 암호화 처리하여 전송합니다.

Q9. SSLVPN에서 VPN 접속 시 필수 소프트웨어는 어떻게 확인하는지요?

고객사에 적용한 케이스는 크게 2가지가 있습니다. 첫 번째는 방화벽 에이전트에서 고객사에서 요청한 소프트웨어에 대한 확인 후 연결하는 방식이고, 두 번째는 방화벽에서 필수 소프트웨어에 대한 정보를 정의하여 에이전트에 알려주면 단말 에이전트에서 이에 대한 정보를 방화벽에 보내줍니다.

Q10. 단말정보를 수집하는 클라이언트에 대한 무결성은 어떻게 확인하나요?

기본적으로 단말정보 수집 클라이언트는 자체 무결성 검증을 수행하고 있습니다. 방화벽에 대한 CC인증 범위에 SSLVPN연결에 사용하는 단말 에이전트를 포함하고 있습니다.

Q10. PC에 설치된 보안솔루션에 대한 운영, 보안관제, 위협제거 등의 서비스도 국내에서 제공받을 수 있나요?

삼성SDS에서는 파견관제, 원격관제, 두 가지 방식을 혼합한 하이브리드형 관제를 통해 문의하신 서비스를 제공해드리고 있습니다. 관제센터는 국내 및 해외 거점 운영을 통해 24시간 무중단 운영됩니다.