Un laboratorio de pruebas de terceros asegura su fuerza de trabajo remota con Hillstone Networks

El Cliente

Fundado en 2002, el cliente es un laboratorio externo con sede en los Estados Unidos que brinda servicios de pruebas, investigación, capacitación y consultoría de alta calidad. Se especializa en muestreo de productos para las industrias alimenticia, ambiental, de agua, de suplementos y nutracéutica. Nuestro cliente se esfuerza por ayudar a sus clientes a obtener datos analíticos precisos, rápidos y confiables, también brinda soluciones totales para ayudar a sus clientes a garantizar la seguridad alimentaria, la calidad del agua y la salud ambiental. El laboratorio de la compañía está acreditado por ISO 17025, y las pruebas se realizan según los métodos estándar de la industria o mediante pruebas desarrolladas y validadas internamente. Ellos presentan a sus clientes cada prueba o serie de pruebas en informes meticulosamente detallados.

El Desafío

El laboratorio de pruebas de terceros atiende a una amplia gama de industrias para cumplir con sus diversos requisitos reglamentarios. Todas las pruebas se realizan en su laboratorio de última generación. A menudo, las pruebas y los informes deben completarse en muy corto tiempo para satisfacer las necesidades del cliente. Al igual que muchas compañías de tecnología, el cliente ofrece a sus empleados horarios flexibles y la opción de teletrabajar a veces para permitir una mayor flexibilidad en el cumplimiento de los tiempos de respuesta tan cortos. Esta tendencia hacia el trabajo remoto es común en toda la industria de la tecnología, especialmente durante desastres naturales, pandemias y otros eventos que interrumpen el negocio.

Sin embargo, para facilitar el teletrabajo, los empleados no solo necesitan acceso remoto a la red corporativa sino también servicios basados en la nube, pero ese acceso debe ser ultra seguro. El trabajo remoto presenta nuevas superficies de ataque que pueden poner en peligro los datos y recursos corporativos críticos. Los dispositivos remotos sin seguridad pueden verse comprometidos por tácticas como la pesca submarina, los troyanos y el malware, y los datos en tránsito pueden estar sujetos a ataques Man-in-the-Middle (MITM) u otros intentos de intrusión. Estas vulnerabilidades pueden traspasar hasta la red corporativa, comprometiendo datos comerciales vitales y otros activos.

Para defenderse de ataques maliciosos, el laboratorio de pruebas buscó una solución segura de acceso remoto para proteger su red y datos dentro de la red corporativa, así como en su nube privada virtual (VPC) de Amazon Web Services. Específicamente, el equipo de informática del laboratorio estaba buscando una solución que abordara cuatro requisitos clave:

1. Acceso remoto seguro a la red corporativa y al entorno de la nube para los empleados, en cualquier momento, en cualquier lugar y en cualquier dispositivo, ya sea de escritorio, portátil o móvil.
2. Seguridad profunda a través de identificación precisa, autenticación y

Un laboratorio de pruebas de terceros asegura su fuerza de trabajo remota con Hillstone Networks

autorización.
3. Políticas de control de acceso hasta la capa de aplicación, así como detección inteligente de posibles amenazas para garantizar los más altos niveles de seguridad.
4. Monitoreo, registro e informes para los administradores de seguridad, con visibilidad granular y análisis de amenazas para detectar posibles ataques y mal uso.

Además, la solución necesitaría proporcionar seguridad integral para la red corporativa, así como para los datos y las aplicaciones que se ejecutan en el entorno de AWS, y proporcionar coherencia y facilidad de administración en ambas plataformas.

La Solución

Después de explorar varias ofertas de seguridad, el cliente eligió la solución de Hillstone Networks que consiste en un firewall de próxima generación E-Series (NGFW) para defender el perímetro de la red corporativa y un NGFW virtual Hillstone CloudEdge para proteger los servicios en la nube de AWS. El equipo en el laboratorio implementó el NGFW físico de la Serie E como la puerta de enlace de la oficinas y CloudEdge como la puerta de enlace VPC dentro de su entorno de nube de AWS.

"La configuración es bastante sencilla. Con CloudEdge, podemos conectar nuestra red corporativa a nuestra instancia de AWS VPC y compartir el mismo conjunto de características de seguridad que se proporcionan en la plataforma física NGFW. Además de acceder a los recursos corporativos, también habilitamos sus características de seguridad adicionales, que incluyen antivirus, prevención de intrusiones y calidad de servicio (QoS) para asegurar nuestro acceso remoto. Además, ahora podemos ver los ataques de amenazas en tiempo real capturados y mostrados en el tablero," dijo el gerente de informática del laboratorio.

Para asegurar los datos en tránsito para su fuerza de trabajo remota, el cliente habilitó los servicios SSL VPN en el NGFW E-Series y CloudEdge, e instaló el cliente VPN de Hillstone (llamado Secure Connect VPN) en los dispositivos domésticos de todos los empleados para un acceso seguro a la red corporativa. Hillstone ofrece una variedad de clientes VPN Secure Connect que admiten sistemas operativos Windows, Mac y Linux, así como Android e iOS para dispositivos móviles, lo que permite que casi cualquier dispositivo remoto se conecte de forma segura y sin problemas.

"Después de pasar la identidad del usuario y la autenticación del dispositivo, nuestra fuerza de trabajo remota ahora tiene acceso seguro a la red interna de la compañía en cualquier momento, en cualquier lugar y desde prácticamente cualquier dispositivo. Rara vez tenemos algún tiempo de inactividad y la productividad ha aumentado," dijo el gerente de Informática.

Al abordar uno de sus requisitos críticos, la autenticación basada en roles es una de las características de seguridad más importantes de esta solución. La solución Hillstone puede interactuar con una amplia variedad de servidores de autenticación, como Active Directory, LDAP, RADIUS y otros, para garantizar que únicamente los usuarios y dispositivos autorizados puedan acceder a los activos de la red. Además, Hillstone Solution incluye una opción para la autenticación multifactor por medio de los token SMS o RSA.

"Descubrimos que una fortaleza clave de CloudEdge es su control detallado en el nivel de usuario, grupo de usuarios o rol. Podemos controlar a qué direcciones IP o subredes puede acceder un usuario determinado, por ejemplo," dijo el gerente de informática. "Sin embargo, este control se extiende más allá de solo los usuarios, tanto a las aplicaciones como a los comportamientos de los usuarios."

Al abordar otro requisito clave para el cumplimiento y la gestión, CloudEdge brinda al cliente un paquete completo de monitoreo, registro e informes ejecutivos y de auditoría. El monitoreo y las alarmas de grano fino, hasta el nivel de aplicación, dispositivo y comportamiento, pueden ayudar a identificar las áreas problemáticas. Los datos se proporcionan en una generosa interfaz de usuario que ofrece una visión general de un vistazo con la capacidad de profundizar para obtener más información y análisis.

La Conclusión

El cliente tenía cuatro requisitos clave cuando buscaba una solución de seguridad para proteger su fuerza de trabajo remota y, en última instancia, su negocio. Hillstone cumplió con los cuatro y con una conexión remota segura a la red corporativa en cualquier momento y en cualquier lugar con cualquier dispositivo. La autenticación y autorización de identidad y dispositivo ayudan a garantizar el acceso adecuado y a proteger contra intentos de piratería. La solución ofrece seguridad en profundidad, especialmente el control de acceso a la capa de aplicación. Mientras tanto, el monitoreo, registro y presentación de informes han ayudado al equipo de seguridad con una visibilidad profunda y recomendaciones prácticas.

Hillstone NETWORKS

Visite **www.hillstonenet.lat** para conocer más
o contacte a Hillstone al **inquiry@hillstonenet.com**