ISONA Secure Access Solution

Sicherer und einfacher externer Zugriff

Die Secure Access Solution von ISONA ermöglicht es Mitarbeitern und externen Dienstleistern, von extern sicher auf beliebige Terminalserver, Server, Webserver usw. im Firmennetzwerk oder in der Cloud zuzugreifen. Klassische Einsatzbereiche sind:
Homeoffice, mobile Mitarbeiter (z.B. Vertrieb, Service), externe IT-Administratoren (IT-System-häuser) usw.

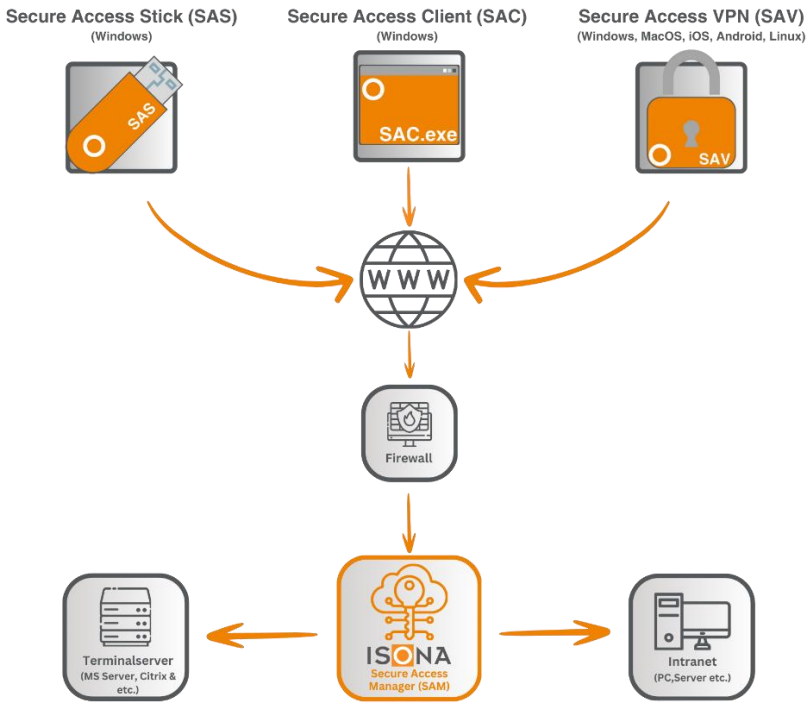
Die ISONA Secure Access Solution besteht aus 3 Produktvarianten:

Secure Access Stick (SAS)

Secure Access Client (SAC)

Secure Access VPN (SAV)

Das folgende Bild zeigt die Integration der Secure Access Solution in eine Kunden-Infrastruktur:



Alle Komponenten der Secure Access Solution werden zentral im ISONA Secure Access Manager (SAM), einer virtuellen Appliance, verwaltet (siehe Bild oben). Der SAM übernimmt dabei die Funktion eines VPN-Gateways, Authentisierungsservers und PKI-Servers, das hinter der Kundenfirewall platziert wird als zweistufiges IT-Sicherheitssystem. Weiterhin fungiert der Secure Access Manager (SAM) als umfangreiches Management-Tool für die drei Komponenten der Secure Access Solution.

Durch die einfache Inbetriebnahme und die bequeme Nutzung wird der Supportaufwand für die IT-Abteilung auf ein Minimum reduziert.
Außerdem ist dies eine kostengünstige Lösung im Vergleich zur Anschaffung von gemanagten Tablets, Notebooks oder PCs.

Gesamtübersicht

Version 1.1

Nachfolgend detaillierte Informationen zu den Komponenten der **ISONA Secure Access Solution**:

Secure Access Manager (SAM)

Der Secure Access Manager (SAM) ist die zentrale IT-Sicherheitskomponente des Gesamtsystems. Er fungiert als VPN-Gateway, Authentisierungsserver, Zertifikatsserver (PKI) und Berechtigungssystem, sowie als zentraler Managementserver für die Secure Access Komponenten. Der Secure Access Manager ist eine virtuelle Appliance, lauffähig auf den meisten Virtualisierungsservern (Microsoft Hyper-V, VMware, VirtualBox, Proxmox, Linux KVM usw.) und wird üblicherweise inhouse beim Kunden oder in der Cloud installiert.

Secure Access Stick (SAS)

Der Secure Access Stick (SAS) erlaubt es, sicher von extern auf Server zuzugreifen. Dieser spezielle USB-Stick benötigt keinerlei Installation oder Adminrechte und hinterlässt auf dem Windows®-Gastsystem keine Spuren, da er in einer abgeschirmten Umgebung (Sandbox) läuft. Sämtliche Software, die der Anwender benötigt um einen sicheren Application-Layer-VPN aufzubauen und auf die vorhandene IT-Infrastruktur zuzugreifen, ist bereits auf dem Stick integriert. Dieser ermöglicht zusammen mit dem Passwort eine hochsichere 2-Faktor-Authentifizierung des Benutzers und ist somit immun gegenüber Angriffen mit Keyloggern oder Viren, die bei den üblicherweise verwendeten VPN-Clients die Passwörter abfangen und damit Cyber-Kriminellen einen unbefugten Zugriff auf Server usw. ermöglichen.
Die Konfiguration und das Management des SAS erfolgt zentral über den Secure Access Manager (SAM).

Secure Access Client (SAC)

Der Secure Access Client (SAC) ist die USB-sticklose Variante des Secure Access Stick (SAS) mit identischen Features. Dadurch wird auch ein Zugang von Windows®-PCs aus ermöglicht, bei denen die Nutzung von USB-Sticks nicht erlaubt ist.
Sämtliche Software, die der Anwender benötigt um einen sicheren Application-Layer-VPN aufzubauen und auf die vorhandene IT-Infrastruktur zuzugreifen, wird nach der Authentisierung ad-hoc von der Secure Access Manager (SAM) auf den Gast-PC geladen und in einer abgeschotteten Sandbox ausgeführt. Für die sichere 2-Faktor-Authentisierung des Benutzers kann je nach Wunsch entweder ein OTP-Token (Schlüsselanhänger) oder eine OTP-App (z.B. Google Authenticator) verwendet werden.
Die Konfiguration und das Management des SAC erfolgt zentral über den Secure Access Manager (SAM).

Secure Access VPN (SAV)

Der Secure Access VPN (SAV) kommt zum Einsatz, wenn der Benutzer Endgeräte im Einsatz hat, die nicht auf Microsoft Windows® basieren wie zum Beispiel Tablets, Notebooks und PCs mit den Betriebssystemen iOS, macOS, Android, Linux usw.
Der Secure Access VPN (SAV) funktioniert auf allen Geräten, für die ein OpenVPN-Client verfügbar ist.
Um die IT-Sicherheit bei diesen Geräten zu gewährleisten, kann man in dem Secure Access Manager (SAM) den VPN-Tunnel soweit begrenzen, dass nur die benötigten Ports und Protokolle freigegeben werden.

Für eine sichere Authentifizierung des Benutzers wird der Secure Access VPN (SAV) ergänzt um eine 2-Faktor-Authentifizierung (2FA) mit einem Einmalkennwort. Für das Einmalkennwort stehen die gleichen Varianten wie beim Secure Access Client (siehe oben) zur Verfügung.
Die Konfiguration und das Management des SAV erfolgt zentral über den Secure Access Manager (SAM).