

STONESOFT

a2cloud Solution for secured authentication and access to cloud

Whitepaper

Combining Modern Authentication Needs with Identity and Access Management

Table of Contents

Introduction	3
The weakest link in the chain	4
A modern multi-method Authentication Solution	6
Cloud interoperability with Federated ID	7
Completing the “big picture” with unified management and centralized information processing	8

Recent trends such as cloud computing and virtualization have defined new challenges for CIOs and CISOs. What was once the definite perimeter for corporate IT has become a thin, vague boundary, often extending outwards to include partners' and even service providers' zones.

A pressing demand exists to precisely outline the separation of duties and privileges, the visibility of applications to users and the verification of security postures. This need clearly goes well beyond the mere validation of credentials.

Introduction

Infrastructural technologies have already helped IT managers to connect and interconnect different physical, virtual and hybrid environments into what is known as the cloud.

Clouds, both private to a company or publicly offered by a service provider, can be considered a) autonomous, and b) interoperable computing environments.

Users connect to the cloud using a huge variety of client devices. This immediately opens the need for universal access on different client platforms, where the only common denominator is the strength of the authentication process.

Cloud computing is subtly bringing uniformity and standardization to the way that applications behave and to the way that different cloud environments interoperate with one another. Naturally, the private and corporate nature of certain cloud environments requires access to legacy applications, thereby inhibiting the uniformity of presentation. But, where standardization is pervading quite consistently is in the role that the cloud plays in IT, since users are accessing the cloud mainly for two reasons: verification of credentials and access to applications.

These usage patterns have created mixed environments where the cloud can play the role of Identity Provider (IdP — if the purpose is to validate user credentials) or a Service Provider (SP — if the purpose is to give access to applications). SP and IdP roles can coexist in the same cloud. Interoperability between an IdP and an SP is normally defined as a Federated Authentication scenario.

Access — The weakest link of the chain

Agility, flexibility and universal access to corporate applications define situations where security needs to be granularized and enforced in layers — infrastructure, applications, connectivity and above all access.

Access is by far the weakest link in the security chain, since it represents the point of contact between two clouds (in the case of federated authentication) and between the users and the data/application they need to operate with.

In such a situation, the security of access process is definitely a focus of the attention of security officers and administrators. This is because compromising the process could undermine the whole security infrastructure, which is in place to protect data against leakage and applications against misuse.

Therefore, there is a pressing demand for solutions combining Identity and Access Management with classic Authentication Systems, featuring contextuality, versatility and adaptability as built-in features. The solution CISOs are looking for must offer the highest level of security, with minimal impact on usability. Thus, unified and centralized control and information processing present a “natural” and complete solution.

The solution that users want to see is access to a needed application that feels as natural as possible using tools they are keen on using, such as tablets or smartphones, without the need to carry dedicated devices. Subtly and transparently as much as possible, they should also go through a process aimed to verify and validate the security posture of the client used and evaluate contextual information from the connection — such as time and IP.

In short, the whole authentication and access process should be ergonomic because it should prioritize people's efficiency in their working environment.

Role	Expectations	Challenges
CISO	Strong Authentication — a solution with minimized costs and maximized manageability and security. Ability to extend trust to the connecting client machine depending on the context of the connection.	Balancing the need for strong authentication against maintenance costs — e.g. hardware tokens that may break, get lost, expire, etc. Notifying end users of the need for passwords/seeds/PINs in a simple yet secure way. Going beyond verification of credentials to verifying contextual security postures.
Operative Administrators	Real-Time Situational Awareness and understanding of success/failures rates when multiple authentication methods are deployed. Ability to analyze all information related to security events, no matter if they are related to network, authentication or client security posture. Ability to document everything using the “incident” concept instead of storing documentation in multiple different locations.	Real time statistics as well as time-based, automatic reporting. Ability to get detailed information to support troubleshooting. Avoiding the need to manually notify users of profile creation or modified authentication information (e.g. when a new seed is generated).
Management	Gain justification to invest in security, avoid security concerns becoming an obstacle to processes/ business.	Gain clear consistent information about working/ non working solutions. Avoid investing in complex solutions (often non-integrated and difficult to manage). Have in place a security system that can integrate with partners’ systems.
End Users	Access to applications and resources in the cloud (private and public) without complex authentication processes. Avoid carrying authentication devices. Positive user experience when accessing corporate applications.	Transparency of security posture verification. Use devices already used for multiple purposes (e.g. smartphones, tablets, mobile phones) for authentication.

A modern multi-method Authentication Solution

Stonesoft's a2cloud Authentication Solution is a balanced mix of products and technologies that embody the ideal implementation of modern multi-method strong authentication and secure access to the cloud.

At the core of the solution is interoperability between two key products of Stonesoft's Network Security Architecture – the Stonesoft Authentication Server and the Stonesoft SSL VPN.

The Stonesoft Authentication Server provides secure remote access to critical data and applications across a given network with a set of four Radius-based servers to implement different authentication methods

Different verticals have different security needs, varying sometimes even on a per-application basis. For example, a bank needs to offer their employees and customers different levels of access to certain applications. Differentiation could be based on authentication methods (some being stronger than others due to multiple factors of strength involved).

These methods are ergonomic, which means they can be used with mobile devices like smartphones that people carry with them at all times. Thus, organizations do not need to make investments in the purchase and/or training of additional hardware, tokens and/or tools.

Applying soft token solutions frees up critical IT resources. Soft tokens are free, they do not get lost and if broken, can be replaced immediately. The same applies to security. Changing unsecured physical devices and hard tokens is expensive with considerable risks involved.

Take the case of RSA. When hard-coded security was compromised the only choice left was to replace all physical devices. While it may be the only reasonable course of action, it takes time and offers no guarantees against it happening again. That's why software-based authentication methods represent the only dynamic way to stay updated and secured.

The Stonesoft Authentication Server is tightly integrated with the Stonesoft Management Center. This allows rapid deployment of a centralized backend authentication system and transparent integration with existing user databases such as MS Active Directory, Novell eDirectory, OpenLDAP and other LDAPv3 compliant systems.

Type-ahead user linking allows for one-click creation of user accounts, Automatic user-linking can be used to allow dynamic generation of user profiles when users attempt login (combined with efficient SMS or mail-based notification of user credentials and/or through One Time Passwords).

Overall ease of management extends to disabling user profiles (when an employee leaves the company) or setting expiry-dates to profiles (for consultants or temporary workers).

Both Stonesoft Authentication Server users and backend user databases can be easily browsed on a graphical user interface, minimizing the administrative burden and boosting efficiency.

Users can also be linked to one or more authentication methods, automatically or manually. This presents many benefits as implementation of an authentication solution often presents a challenge in the administrative burden of importing/accessing/defining huge numbers of users.

Take the case of a company needing to deploy internal access to email with password-based authentication and IPSec mobile VPN for external employees with a stronger authentication method (e.g. OTP to phone). An ideal solution allows the generation of a user profile immediately as the user tries to authenticate with either of the two methods — enabling both for that user. This minimizes administrative costs, improves efficiency and shortens the overall solution's implementation time.

The Stonesoft SSL VPN enforces security of access through a combination of local authentication techniques. It combines the strength and number of factors of each method with the number of methods.

For example, a user can start the access process by presenting a digital certificate. Once this has been validated, the user is prompted for a password and an additional One Time Password is delivered to his mobile phone via SMS.

Once the user is allowed in, access to applications is conveniently available through Single Sign-On techniques — for both web and legacy applications, including Remote Desktop, Fileshare Access or SSH/Telnet.

This relieves the user from needing to remember multiple passwords or re-typing the same information multiple times. SSO also minimizes errors in accessing applications as well as the time spent on accessing them — improving the overall user experience. Once properly authenticated and trusted, the user is given smooth access to where his level of trust allows.

During a session, a firewall instance can grant that only wanted traffic is allowed to/from the client and a trace removal technique ensures that no important data gets left behind should the session is conclude with logout.

A winning combination

The combination of the two products can be used to achieve maximum security of access to the cloud through multi-factor and multi-method authentication and verification of the connecting client's security posture.

Both StoneGate Authentication Server and StoneGate SSL VPN can be implemented in mirrored configuration to ensure resiliency and high-availability in the most demanding environments.

Cloud interoperability with Federated ID

Federated ID techniques are becoming increasingly popular, concurrent with Cloud Computing architectures and scenarios becoming more important for Service Providers. The purpose of a federated authentication scenario is to offer agile application deployment in the service provider's cloud(s) while leaving authentication to the customer. Losing control and sacrificing the strength of authentication has been a major obstacle that organizations experience with cloud-based services, especially when they would like to use multiple cloud services and applications.

However, Single Sign-On operations and user profiling remain possible thanks to assertions securely sent from Identity Providers to Service Providers – once the user has been authenticated.

With Federated ID, the application or service provider may delegate the authentication process back to the end-user. The service provider does not need to maintain and administer user account information. This helps improve the time-to-market for cloud-based services and applications, as the app does not need to define user profiles. And nobody needs to be burdened with importing user profiles.

Additional advantages for the end users are being able to authenticate using any method they prefer - and to access an application in the cloud as easily as they would an application in the corporate network.

From the CISO perspective, the company accesses the cloud application while keeping authentication safely “at home.” That is, they retain control over the authentication process, relying on the cloud app service provider just for the operative benefit of having an app in the cloud — reduced maintenance, immediate and easy upgrades, no local implementation, and so forth.

The Stonesoft a2cloud Solution lets administrators configure the components to act as an Identity Provider (StoneGate Authentication Server and StoneGate SSL VPN) and as a Service Provider (StoneGate SSL VPN). Thanks to the open standard nature of such interoperability, the counterpart in a federated authentication scenario can be any third party solution compatible with the supported standard protocols, such as SAML 2.0 and ADFS.

Completing the Big Picture: Unified management and centralized processing

The ability to centrally process information related to security events is important in ensuring the ability to drill into the data while moving from meaningful “big pictures” made of statistical information, geotagged graphs and maps to logs with precise details about specific events.

Such “situational unawareness” is an all too common state of affairs resulting from dispersed information, which could lead to multiple negative scenarios. These range from inefficient troubleshooting to longer reaction times to longer time to market, and excess vulnerability from advanced attacks such as AETs.

When negative security events happen (e.g. when a user gets locked due to multiple authentication failures or violation of a security policy), it is important to have an alerting mechanism, complete with escalation and historical data. Not just for smooth handling of the situation, but for both regulatory compliance and auditing purposes.

Further negative scenarios include users trying to authenticate through guessing passwords— if the user gets locked, administrators are alerted of the violation attempt. Additionally, as users may have difficulties in understanding or adopting a given method, the administrators may decide to disable it or use a less complex method.

Knowing this problem exists in the first place is possible due to the real time statistics and graphical reporting of the Stonesoft Management Center, available as a multiplatform software solution included in each Stonesoft Authentication Server license.

Built on solid architectural foundations, the SMC offers unified management capabilities for all Stonesoft Network Security Platform engines, from the Stonesoft SSL VPN, Stonesoft Firewall/VPN to the Stonesoft IPS, plus the ability to collect logs of third party servers and engines and enhance them with advanced reporting and log analysis capabilities.

The combination of the Stonesoft Authentication Server, Stonesoft SSL VPN and Stonesoft Management Center defines the ideal solution for every modern authentication needs, while simplifying the security of cloud computing environments.

STONESOFT

Stonesoft Corporate

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 713 49

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax. +1 770 6681 131

Copyright 2012 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.