SOLUTION BRIEF

Fortinet and CASQUE Security Solution

Enerprise Owned and Controlled High-grade Identity Assurance

Executive Summary

The inherent vulnerability with existing multi-factor authentication products is that they rely on fixed secrets. This could be an embedded key that manufacturers insert in password generators or in private keys that attest credibility. If found out by discovery, by quantum factorization, or more likely through disclosure from a privileged insider, security gets compromised. Software-only solutions that apply machine learning to define usage profiles and deny access on exceptions have intrinsic flaws—the most permissive become the easiest targets and administrative teams get involved to handle legitimate exceptions. But how are these policed?

CASQUE and Fortinet recently established a technology partnership to address the above challenges. The joint solution protects the enterprise's digital crown jewels, prevents insider collusion, and acts as a potent deterrent to user misuse and so reduces the overall risk to the organization.

Joint Solution Description

CASQUE is based on a Challenge-Response Protocol with the user needing a secure hardware chip to make the response that enables dynamic key change. There are many manifestations of the handheld Token; the most popular being an EAL6 rated secure contactless smartcard. There are two main software components; the first enables the customer to populate Tokes with initial key sets and the second is the CASQUE Server that provides federated authentication services to the FortiGate gateway.

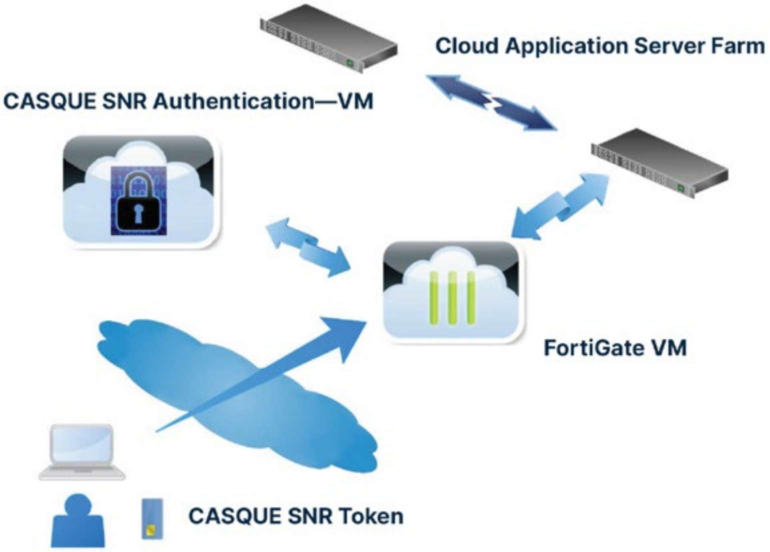

Figure 1: Fortinet and CASQUE joint solution.

Joint Solution Components

- Fortinet FortiGate Next-generation Firewall (NGFW)
- CASQUE SNR Authentication, Token

Joint Solution Benefits

- Allows customers—not third parties—to own and manage their identity access
- Enables customers with secure access to web/mobile applications hosted across on-premises and multiple cloud environments
- Denies users the ability to repudiate illegal access, thus proving a powerful deterrent
- Removes a substantial segment of threat vulnerability and prevents disclosure by corrupt insiders; moreover, tokens cannot be cloned

Solution Components

CASQUE SNR

Distributed Management Systems has developed CASQUE, a radical, Identity Assurance Technology. CASQUE is the only

multi-factor authentication technology that does not rely on fixed secrets, so there is nothing for a hacker to target or for an insider to disclose. CASQUE, therefore, removes a whole segment of threat vulnerability. Moreover, because it denies users possible reasons to support their repudiation of access, it acts as a powerful deterrent against collusion.

FortiGate: Next-generation Firewall (NGFW)

FortiGate enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the cloud. FortiGate enterprise firewalls leverage purpose-built security processors (SPUs) that deliver scalable performance of advanced security services like threat protection, secure sockets layer (SSL) inspection, and ultralow latency for protecting internal segments and mission-critical environments.

The FortiGate NGFW provides automated visibility into cloud applications, Internet-of-Things (IoT) devices, and automatically discovers end-to-end topology view of the enterprise network. FortiGate is a core part of the Security Fabric and validated security protects the enterprise network from known and unknown attacks.

Use Cases

Current activities in many organizations include both transforming legacy systems as well as developing new applications into cloud deployments with the capability of mobile access. With CASQUE, only the customer generates and controls keys. Since FIDO2 and Google Titan fobs have no association with users, even lost devices will work.

Most users want access from a set of different devices—mobile, laptop, desktop with different operating systems—Android, Windows, and Linux. CASQUE provides a universal solution by delivering the challenge directly to a mobile when the mobile is the client, or displaying it as a QR coded image with the mobile acting as a surrogate reader.

CASQUE is predicated on the Fortress design—extensive boundary walls but with the inner keep, containing the digital crown jewels, having the strongest and thickness walls—the CASQUE barrier. It does not seek to replace existing security provisions but to strategically augment it. It is not recommended to use a known vulnerable method to protect administrator access which, if it can be breached, results in the ruination of the entire integrity of the cloud platform including exposure of the crown jewels.

About CASQUE

CASQUE Technology has been developed by Distributed Management Systems, a private company owned by its Directors and based in Lancashire, England. CASQUE has granted US and EU patents and is certified by UK National Cyber Security Centre as suitable for Secret. Learn more at https://www.casque.co.uk.

August 27, 2021 4:17 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:sb-FA-fortinet-and-casque-security-solution:sb-FA-fortinet-and-casque-security-solution_2021

447691-0-0-EN