Datasheet

Viettel Enterprise Mobility Suite
(VCS M-Suite)

viettel security

WHAT IS ENTERPRISE MOBILITY SUITE (M-SUITE)?

In the new era of 4.0 industrial revolution in which digital technologies developed dramatically, the field of information security is a matter of great concern. Information security threats are increasing and whether each entity is truly secure and each endpoint connection is truly reliable is a question posed to the field of cybersecurity today.

Traditional security methods are centralized, respond slowly and operate on a sense of misplaced trust or provide excessive access to an entity's entire network pose a challenge in the face of volatility of current network security issues.

Traditional VPNs or firewalls are no longer suitable for a borderless digital world, which requires a user-centric security model to adapt to the situation.

• **VCS M-Suite** is a solution that provides network security during remote connection process and remote access, built on the requirements of maximizing information security for businesses.

• **VCS M-Suite** is a product with a fresh and modern approach to security for remote connection, which is the application of the SDP (Software Defined Perimeter) protocol. SDP is a one-to-one network security model between users and the resources they access.

• **VCS M-Suite** adheres to the core principles in the field of cybersecurity, on par with similar products in the world in the digital security industry.

SOLUTION FEATURES

The VCS M-Suite solution implements the International Standard Software-Defined Perimeter (SDP) protocol announced by Cloud Security Alliance, providing maximum support safely and professionally for end users in their remote access process, with the following main features:

Flexible access policies

VCS M-Suite replaces static access rules with direct authorization through flexible access policies tailored to individual use cases. Administrators can easily change security policies based on user activities, locations and usage times. The specific access controls ensure that end users only access the necessary resources required to do their tasks securely and consistently, and automatically eliminate the elements of human errors caused by users.

Individual security perimeter

VCS M-Suite uses each user's data in real time according to policies to create an individual security perimeter. This ensures that all devices are verified and authorized before accessing any resources. After the user identified, VCS M-Suite will create a private secure path that only allows data to be transferred from the device to the required resources.

Protection against cyber attacks

VCS M-Suite is built as a security layer to hide the infrastructure behind; only verified users can access the system. This security layer is invisible to vulnerability scanning attacks and is encrypted to increase system security level. Gateways and Controllers are completely concealed so they cannot be probed, scanned or attacked. This helps preventing network reconnaissance activities as well as direct network attacks on system resources.

Protection against unauthorized access

VCS M-Suite can protect both devices and resources against unauthorized connections by securing the device against incoming connection requests. Decentralization of connections to internal resources can be carried out without any concern for unauthorized users on the internal network and without affecting the traffic of data transmission in the internal network.

Flexible deployment

VCS M-Suite is designed to work on both cloud computing and physical servers. VCS M-Suite provides consistent access controls across environments of varying sizes. Administrators can connect users to internal applications seamlessly through the access policies of VCS M-Suite.

OUTSTANDING ADVANTAGES

VCS M-Suite is a powerful security platform that provides a comprehensive SDP solution, is capable of securing any applications, on any platforms, in any locations with three main focuses:

Identity center

VCS M-Suite is designed based on user and device identifications instead of IP address, building multidimensional user's profile or device and granting permissions to users prior to the access request.

Authorization model

Enforce access model security through permissions or policies; apply the principle of least privileges to users to reduce unauthorized access or the risk of network attacks.

Flexible deployment

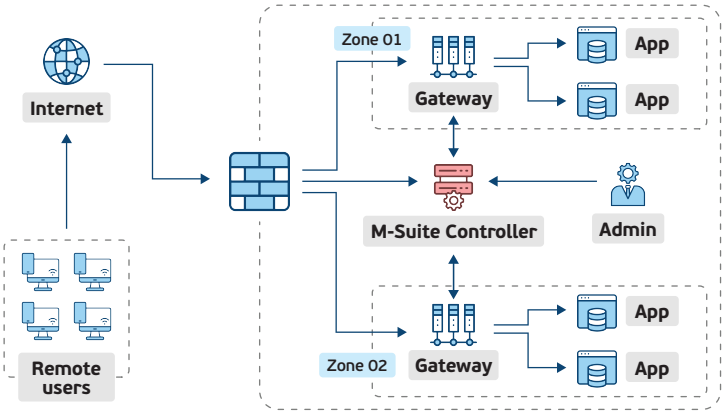
VCS M-Suite is built for easy deployment on physical machines or cloud computing platform, setting up or upgrading each functional module flexibly according to business needs.

Datasheet

Viettel Enterprise Mobility Suite
(VCS M-Suite)

viettel security

ARCHITECTURE OF VCS M-SUITE



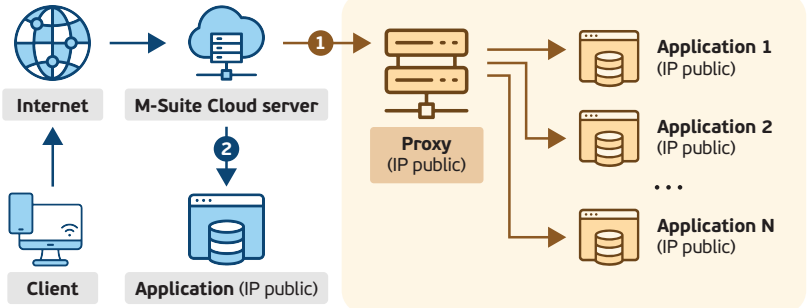
VCS M-SUITE CONTROLLER

A centralized authority, responsible for determining which devices and users are allowed to connect. Alter the device and user authenticate successfully, results will be sent to the Gateway.

VCS M-SUITE GATEWAY

Gateway is where users and devices are allowed or denied access to internal applications. It has the function to create proxy connections from Agent client to application servers.

M-SUITE CLOUD CONNECT



1 Proxy connection option
- Do not publicize internal applications to the Internet.
- Only need 1 public IP for all applications.
- Encrypt 2-way SSL traffic between M-Suite Server and Proxy.

2 Public connection option
- No additional resources needed.
- No additional installations required.
- TCP & UDP support.

FEATURE		Basic	Advanced
Identity Management	Identity management	✓	✓
	Authentication - Local/ LDAP	✓	✓
	Authentication - Restful API		✓
	Multi-factor authentication - TOTP	✓	✓
	Multi-factor authentication - SMS/ Email/ FIDO2		✓
	Internal Directory Synchronization (LDAP)		✓
	Authentication Policy Management		✓
Access Management	Support TCP protocol	✓	✓
	Support UDP protocol		✓
	Approvals for device access management		✓
	Access rights management by user	✓	✓
	Access rights management by group/organization/IP/device/session time/reliability		✓
	Network configuration management		✓
	Application information management	✓	✓
	Access policy management: URI, Traffic, Maximum Speed, Method, Whitelist, Block Network, Data Protection		✓
	Data usage behavior monitoring - TCP	✓	✓
	Data usage behavior monitoring - HTTP/ HTTPS		✓
	Single packet authorization support for Anti-DDoS	✓	✓
Trust inferer	Assess reliability according to baseline		✓
Device Management	Device information viewing: user information, hardware information, application list	✓	✓
	Set baseline for the device		✓
	Mobile device security profile applying: application installation policy, security configuration requirements on device		✓
	Mobile device command: get location, delete data, take photo, lock device		✓
Privileged Access Management	SSH access management: log activity, filter allowed commands		✓