



搞資安， 帳號與特權管理落實了嗎？

Teddy 莊永杰

你們所了解的零信任？



FORTINET 的四個零信任

裝置零信任



FortiClient
ZTNA

Fortigate

- 升級端點加 Fortigate 即可做零信任
- 持續不中斷地檢查
- 端點可啟用防毒機制

身份零信任



Fortiauthenticator

Fortitoken

- 單一認證 (SSO)
- 支援 OTP
- FortiToken 買斷制
- 整合 AD, SAML 等認證
- 已與 O365 等機制整合

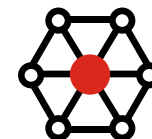
特權零信任



FortiPAM

- 單一入口控管人員
- 統一管理特權帳號
- 內建側錄功能
- 整合 DLP, 防毒等功能

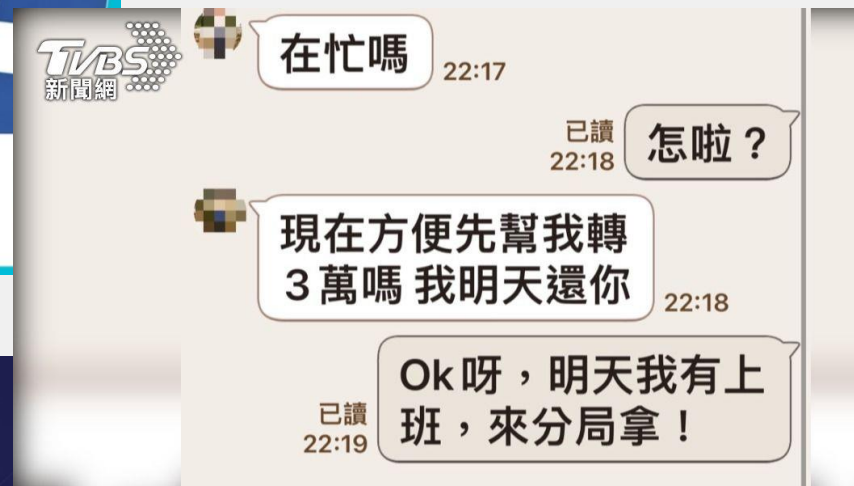
全域零信任



FortiSASE

- 單一資安平台
- 可與既有 Fortinet 整合
- 台灣在地機房
- 計算方法簡單

帳密外洩後的風險...

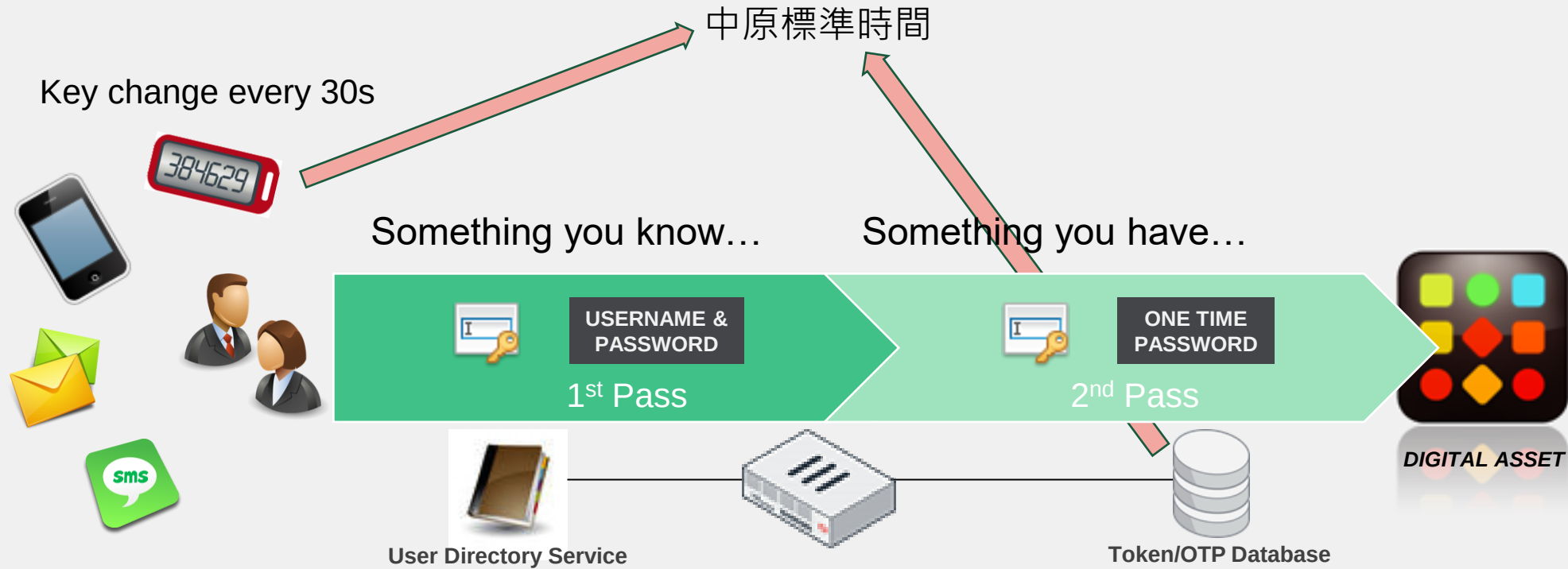


- 每三個月更換密碼
- 高強度密碼設定
- 沒有整合統一認證機制

帳密認證的進化：雙因子認證 & 無密碼 FIDO 認證



雙因子認證 (Two factor Authentication)



FortiToken – Two-Factor Authentication

Multiple Token Options, Easy to Use and Deploy

Perpetual License

FortiToken Mobile App Simplifies User Input to “Click to Accept”

Hardware Tokens Available – to Suit All Use Cases

Self-Service Portal for Guest Access and BYOD

Simple **Deployment** options

Perpetual Licensing – No Ongoing Fees for Locally Managed FortiToken

384629

FortiToken Mobile



Multi platform OATH OTP application with push notification of login attempts and one tap approval

FortiToken 200B / 200BCD



Durable, large display, OATH OTP token with FortiGuard activation or optional encrypted activation file.

FortiToken 220



A mini credit form factor OTP token

FortiToken 300



- Driverless USB Device
- FIPS-140 compliant
- Economical PKI authentication. Use with cryptography apps, VPN, web-based apps

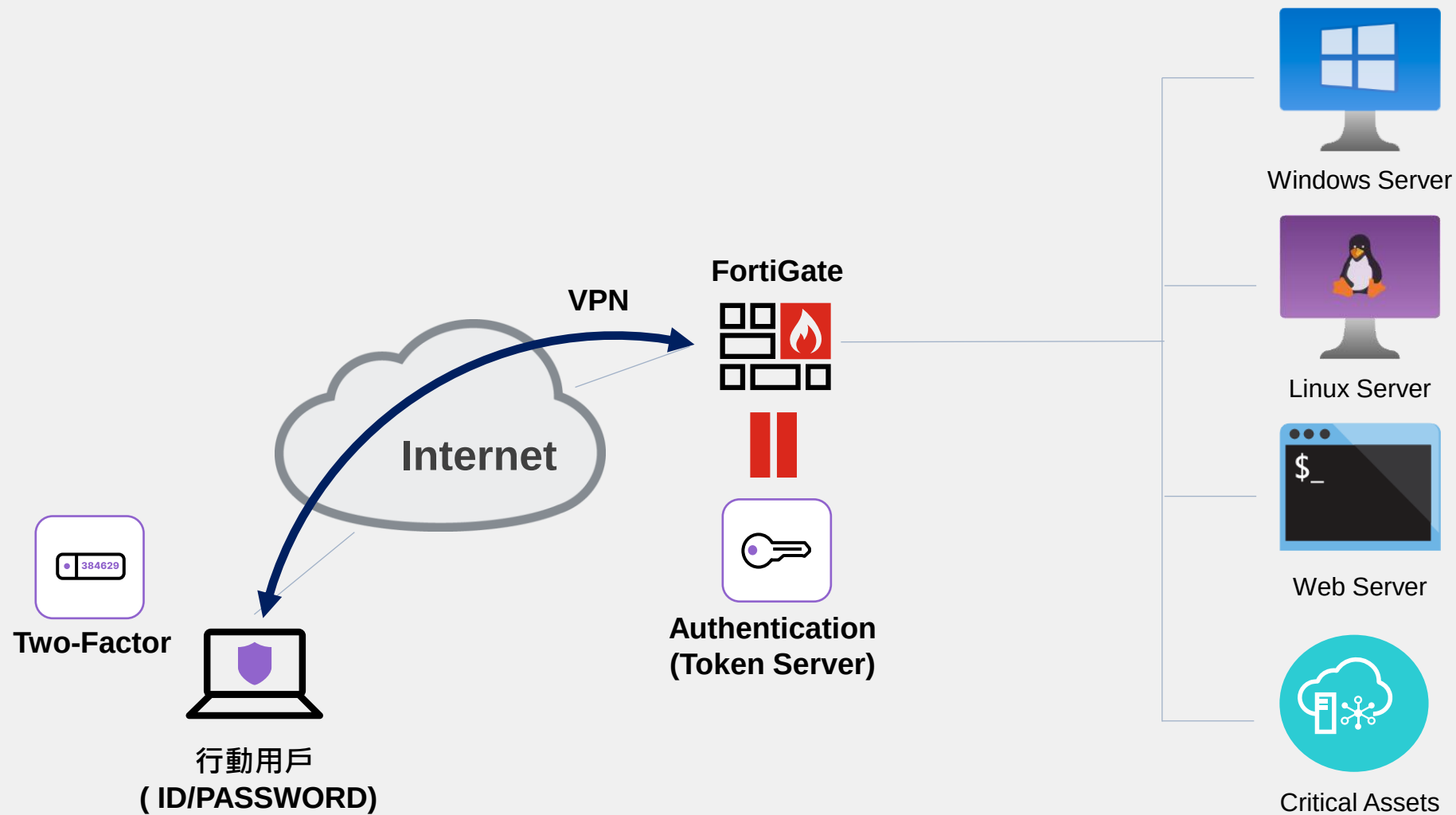
FortiToken 400



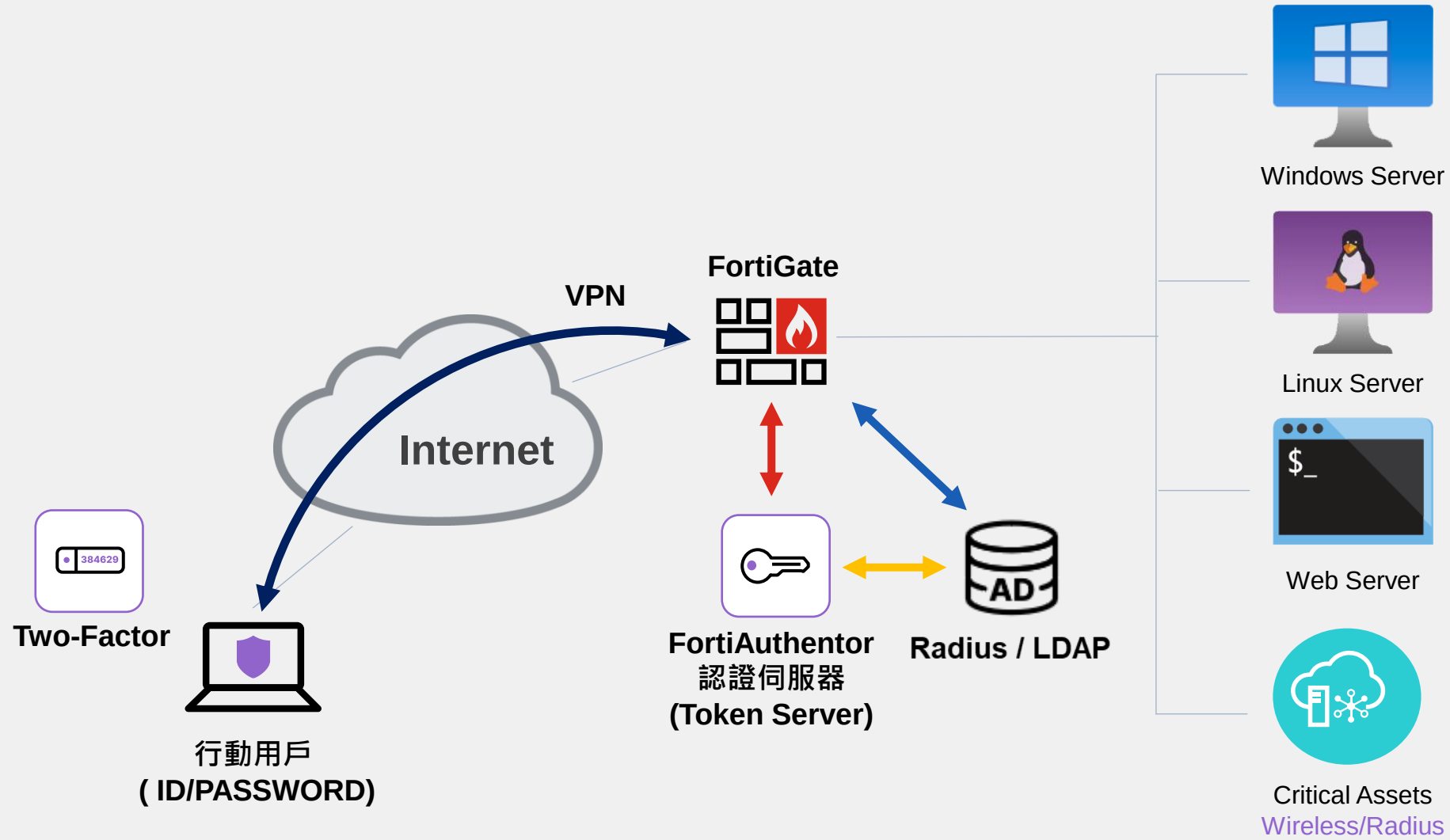
- FIDO certified
- Passwordless security key
- Use with SSL/VPN, SaaS, or FIDO2 supported browsers



運用場景一：VPN with FGT two factor



運用場景二：FGT with FAC integrate



FortiAuthenticator 功能



Strong Authentication and Authorization

- RADIUS and LDAP Authentication
- External LDAP integration
- Hardware, mobile, SMS and e-mail tokens
- REST API



802.1X Port Access Control

- IEEE802.1X supporting EAP-TTLS, EAP-TLS, PEAP, EAT-GTC
- MAC address bypass



Certificate Authority

- X.509 Certificate signing (CA)
- Certificate distribution via SCEP
- User – Certificate binding
- Revocation

Single Sign On

- Active Directory Polling
- Single Sign-on Portal
- Embedded widgets
- FortiClient User ID
- Carrier RADIUS Integration





常見權限帳戶 使用與管理痛點

一個共享的管理員帳戶

無法進行有效稽核，究竟是誰？人是誰殺的？

管理員帳戶與個人帳戶綁定

傳統常用的方法，安全風險大，
個人帳號失守，整體安全失效。

拆分管理帳號與工作帳號

實務上，難以實踐，並且會導致漏洞。



特權帳號管理 - 1H、2W、3Safe



Who

帳號是誰要用

驗證使用者身分為合法

How

用多久、能用什麼

分級審核制度
最小權使用權限範圍

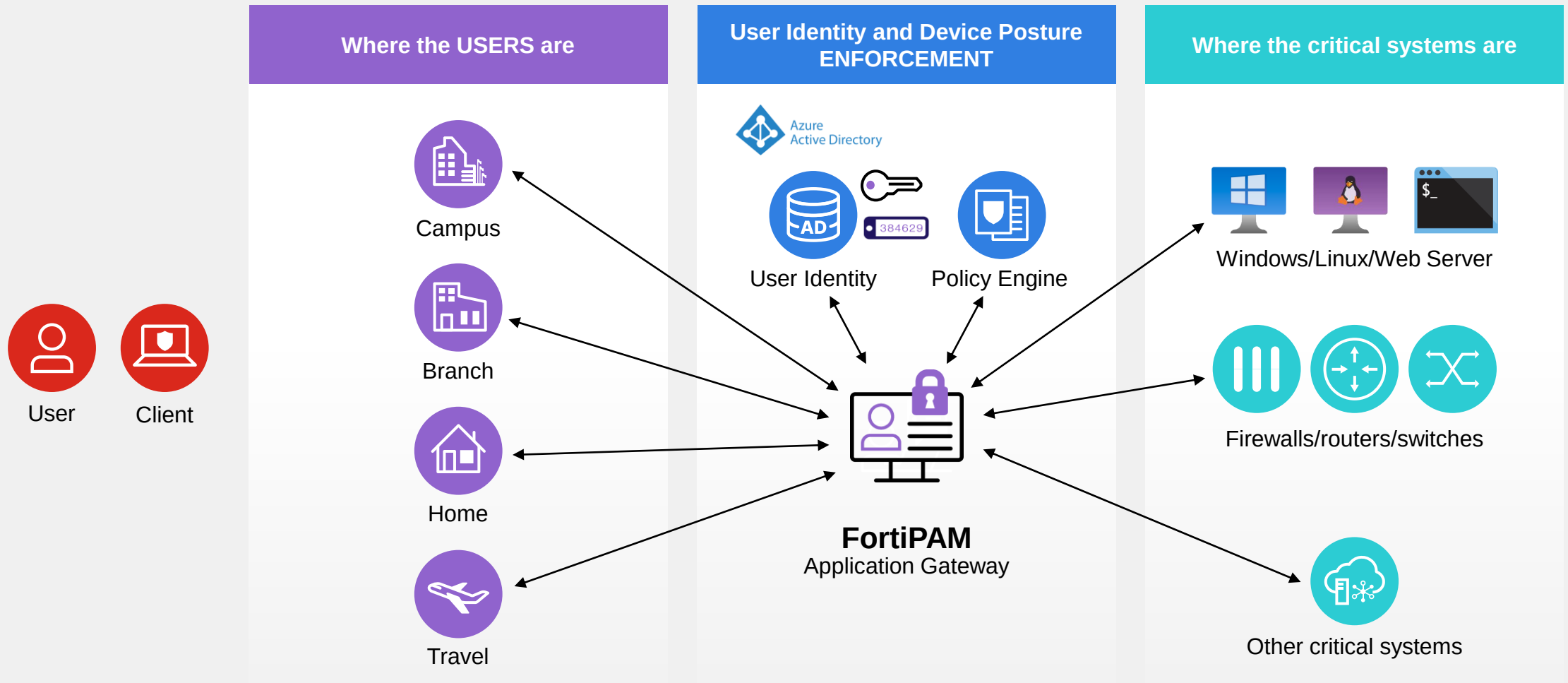
What

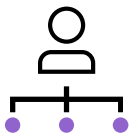
帳號做了什麼

活動監控、記錄、監測

FortiPAM as Application Gateway

The components of FortiPAM





FortiPAM - 用戶管理 (Who)



用戶認證管理

- 本地帳戶
- 遠端帳戶：RADIUS
- 遠端帳戶：AD/LDAP
- 遠端帳戶：SAML IdP



彈性的多因子密碼機制

- 多因子驗證機制(MFA)
 - Email OTP
 - FortiToken
 - FortiToken Mobile



進階的安全強化機制

- 來源位址確認
- 連線時間限制
- 零信任存取架構



FortiPAM - 審核與控管 (How)

存取憑證流程審核

- 組織可依需求決定審核流程。
- 啟用後，使用的用戶，要獲得授權後才能連線主機。
- 存取流程審核流程最多 3 層。
- 每一層至少一位授權者。
- 核決授權者角色，可為 User 或 Group 成員。

Edit Approval Profile

Name

Single-Approval

Number of Approval Layers ?

One

Two

Three

Description

Layer-1 Settings

Required number of Approvals

2

Approvers

 sally



Approver Groups

 MgmtApprovals





FortiPAM - 審核與控管 (How)

權限控制 - 誰可以連線

✓ 管控政策

- Inherit Policy - **Enabled**:
由上至下層群組套用一致的權限原則
- Inherit Policy - **Disabled**:
可透過自訂套用至不同的子群組。

✓ 使用權限

- 可套用至使用者及群組。
- 可細緻設定連權限：
 - view, list, add, edit, owner

Edit Secret Folder

[Edit Folder](#) [Refresh](#)

Name:

Parent Folder:

Inherit Policy: ☐

Secret Policy:

Inherit Permission: ☐

User Permission:

ID	Users	Folder permission	Secret Permission
1	admin	Owner	Owner

Group Permission:

ID	Groups	Folder permission	Secret Permission
No results			

Edit User Permission

Users:

Folder Permission:

Secret Permission:

Edit User Permission

Users:

Folder Permission:

Secret Permission:





FortiPAM - 監控與紀錄(What)

凡走過必留下足跡



會話錄影紀錄

- 支援全會話錄影。
- 會話使用期間滑鼠點擊、鍵盤活動紀錄。
- 影像保留紀錄政策。
- 可自定義會話錄影保留政策。



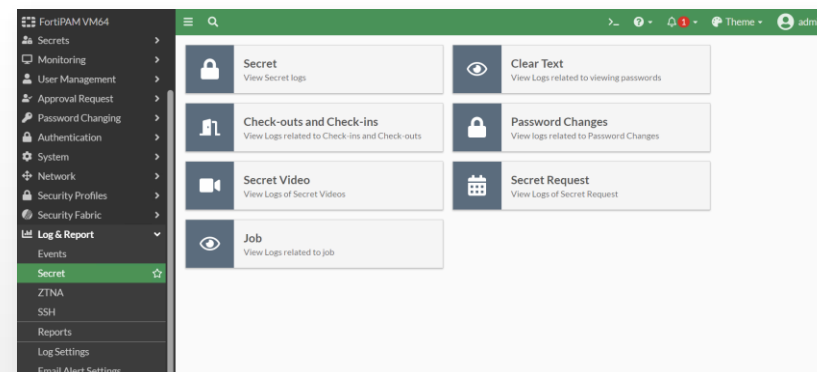
紀錄

Events

- 系統紀錄。
- 使用者活動紀錄。

Logs

- 存取紀錄。
- 簽出、簽入紀錄。
- 操作紀錄。





FortiPAM - 安全強化 (Safe)

Secure File Transfer, Securing Secrets and Monitoring



檔案安全傳遞

檔案交換惡意威脅偵測

- 可聯動 FortiSandbox 、
FortiNDR 偵測已知、未知
Zero-day 惡意程式。
- 支援 WinSCP 、 WinSMB 。



系統資料 安全保護

TPM 加密機制

- TPM in Hardware Models 。
- vTPM in Virtual Machine 。

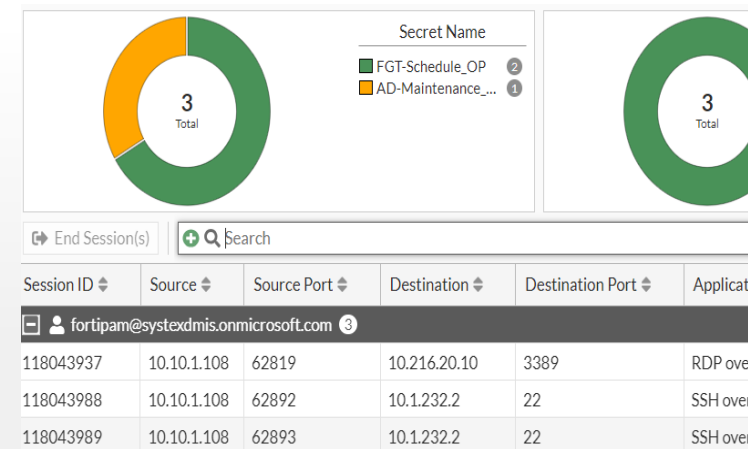


Trusted Platform
Module



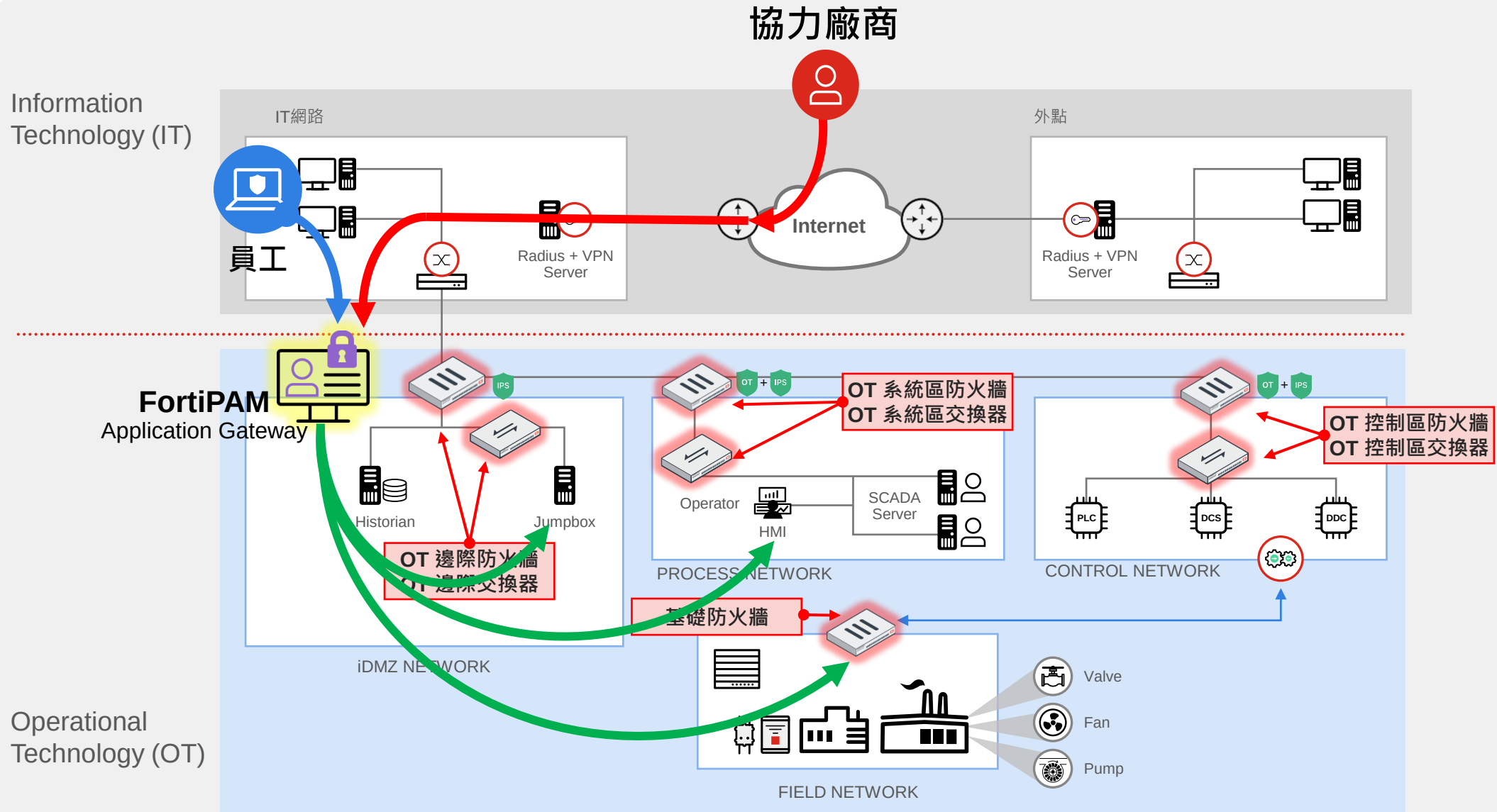
監督

- SSH 風險性指令控制 。
- 使用者及連線監控 。





安全的使用接入點





安全協定保護 - Web RDP

Launch Progress

> Select Launcher

Getting Info

Launching

Done

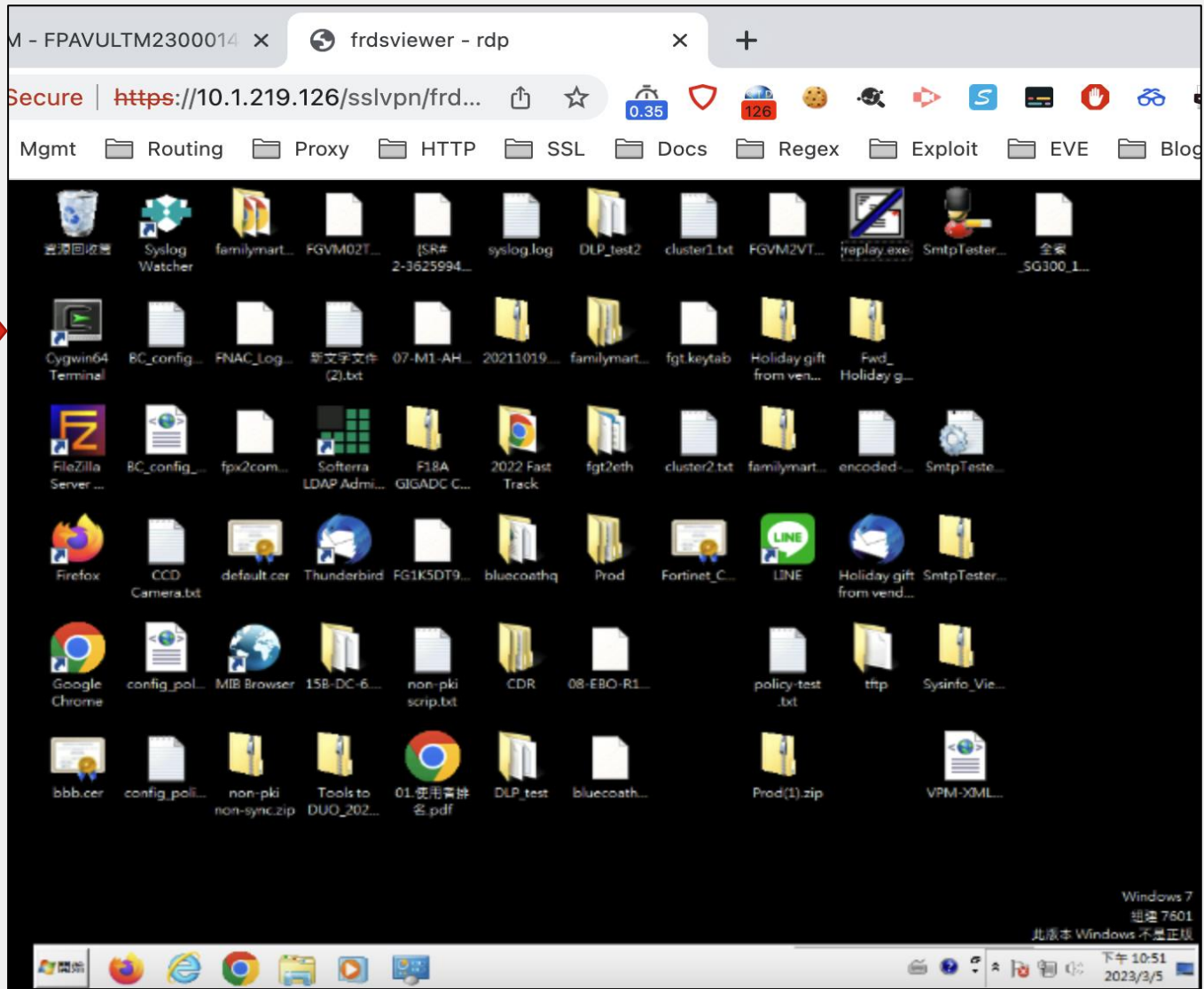
Launch Secret: JUMPBOX

Remote Desktop-Windows

Web RDP

Launch

Cancel



保護 RDP 協定

“避免直接暴露”





操作的安全性 - 指令過濾器

保護系統操作 “避免無意或蓄意的指令”

te Edit Delete				
Type ▾	Pattern ▾	Action ▾	Log ▾	Alert ▾
Regex	^ex[a-z]*[\s]*[a-z,-]*reset	Block 	Enable	Enable
Regex	exec[a-z,\s]*reb[a-z]*	Allow	Enable	Enable

```
FGVM02TM23000965 # get sys status  
Version: FortiGate-VM64 v7.2.4,build1396,230131 (GA.F  
Virus-DB: 1.00000(2018-04-09 18:07)  
Extended DB: 1.00000(2018-04-09 18:07)  
Extreme DB: 1.00000(2018-04-09 18:07)  
AV AI/ML Model: 0.00000(2001-01-01 00:00)  
IPS-DB: 6.00741(2015-12-01 02:30)
```

 FG80F-LAB2_Spoke \$ **execute factoryreset**
The command is not allowed to execute. Please check with your administrator.





紀錄資料

Secret
View Secret logs

Check-outs and Secret Video
View Logs related to Secret Video

Job
View Logs related to Job

Secret Video Details

Search

Date/Time	Token Id	Secret name	User
2023/03/05...	2904276946	VMware ESXi	a
2023/03/05...	2904276946	VMware ESXi	a
2023/03/05...	2899492783	VMware ESXi	a
2023/03/05...	2899492783	VMware ESXi	a
2023/03/05...	2874457834	FGT-VM	a
2023/03/05...	2874457834	FGT-VM	a
2023/03/05...	2851061257	FGT-VM	a
2023/03/05...	2851061257	FGT-VM	a

Log Details

Video

```
FGVM02TM23000965 # get sys status
Version: FortiGate-VM64 v7.2.4, build1396, 230131 (GA.F)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
IoT-Detect: 0.00000(2022-08-17 17:31)
Serial-Number: FGVM02TM23000965
License Status: Valid
License Expiration Date: 2024-02-02
VM Resources: 1 CPU/2 allowed, 1994 MB RAM
Log hard disk: Available
Hostname: FGVM02TM23000965
Private Encryption: Disable
Operation Mode: NAT
--More--
```





Daily Report

每日報表整理連線的時間、次數與人員的連線紀錄

Top Failed Password Verification by Secret Name and Reason

#	Secret Name	Reason	Totals
1	RDP250 (*a32761)	connection-error	5
2	FTP (*5c7249)	connection-error	1
3	RDP250 (*a32761)	login-auth-error	1

Top Failed Password Verification by Secret Name, User and Reason

#	Secret Name	User Name	Reason	Totals
1	RDP250 (*a32761)	admin	connection-error	5
2	FTP (*5c7249)	admin	connection-error	1
3	RDP250 (*a32761)	admin	login-auth-error	1

Clear Text View

Summary	Stats
Total # of Views	14

Top Clear Text View by Secret Name

#	Secret Name	Total # of Views
1	RDP250 (*a32761)	6
2	SMB (*37315b)	5
3	FTP (*5c7249)	2
4	RDP (*e88a77)	1

Top Clear Text View by Secret Name and User

#	Secret Name	User Name	Total # of Views
1	RDP250 (*a32761)	admin	6
2	SMB (*37315b)	admin	5
3	FTP (*5c7249)	admin	2
4	RDP (*e88a77)	admin	1

Schedule-default-2023-05-17-000100

5 of 7

Secret

Secret Launch Success

Summary	Stats
Total # of Launches	39
Total Duration	02h 12m 22s

Top Secret Launch Success by Secret Name

#	Secret Name	Total # of Launches	Total Duration
1	FTP (*4597ed)	9	02h 01m 48s
2	7.A_SSH (*36ab5c)	8	06m 29s
3	FTP (*5c7249)	6	01m 23s
4	FTP (*45ba47)	4	55s
5	FTP (*c1a030)	4	16s
6	RDP250 (*a32761)	3	55s
7	SMB (*5c7831)	2	11s
8	RDP (*e88a77)	2	07s
9	FTP (*3999bb)	1	18s

Top Secret Launch Success by Secret Name and User

#	Secret Name	User Name	Total # of Launches	Total Duration
1	FTP (*4597ed)	admin	9	02h 01m 48s
2	7.A_SSH (*36ab5c)	admin	8	06m 29s
3	FTP (*5c7249)	admin	6	01m 23s
4	FTP (*45ba47)	admin	4	55s
5	FTP (*c1a030)	admin	4	16s
6	RDP250 (*a32761)	admin	3	55s
7	SMB (*5c7831)	admin	2	11s
8	RDP (*e88a77)	admin	2	07s
9	FTP (*3999bb)	admin	1	18s

Password Change

Summary	Stats
---------	-------



FortiPAM-VM sizing guidelines

The following table provides FortiPAM-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

Users	Virtual CPUs	Memory	Storage
-------	--------------	--------	---------

20 - 1000

Log and video disk size guidelines

The following tables provide FortiPAM log and video disk size guidelines.

Disk	Required
Log (minimum)	10 GB
Video (minimum)	10 GB

Recording Resolution	From the dropdown, select a resolution for the PAM video recordings: 480p 720p (default) 1080p
Recording FPS	Enter the PAM video recording frame rate (default = 2, 1 - 15).
Recording Color Depth	From the dropdown, select a color depth: 24 Bit Color Depth (default) 32 Bit Color Depth
Recording Key FPM	Enter the PAM video recording key frame rate per minute (default = 1, 1 - 60).

Video length	Video file size
1 hour	250 MB



FORTINET 的四個零信任

裝置零信任



FortiClient
ZTNA

Fortigate

- 升級端點加 Fortigate 即可做零信任
- 持續不中斷地檢查
- 端點可啟用防毒機制

身份零信任



Fortiauthenticator

Fortitoken

- 單一認證 (SSO)
- 支援 OTP
- FortiToken 買斷制
- 整合 AD, SAML 等認證
- 已與 O365 等機制整合

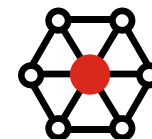
特權零信任



FortiPAM

- 單一入口控管人員
- 統一管理特權帳號
- 內建側錄功能
- 整合 DLP, 防毒等功能

全域零信任



FortiSASE

- 單一資安平台
- 可與既有 Fortinet 整合
- 台灣在地機房
- 計算方法簡單



FORTINET®