DATA SHEET

FortiProxy™

FortiProxy 400E, 2000E, 4000E and VM

FortiProxy is a secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention and advanced threat protection. It helps enterprises enforce internet compliance using granular application control. High-performance physical and virtual appliances deploy on-site to serve small, medium and large enterprises.

SSL Inspection

Powerful hardware that can perform SSL inspection to effectively remove blind spots in encrypted traffic, without compromising on performance.

Protection against sophisticated web attacks

Integration with proven FortiGuard Threat Intelligence Service and FortiSandbox Cloud to protect enterprises from the latest sophisticated threats.

Authenticated web application control

Granular application control policies to restrict access to social websites using user or group identity.

Highlights

- Advanced Protection against threats
  - Integration with FortiGuard Threat Intelligence Service
  - Web, DNS filtering and application control
  - Integration with FortiSandbox cloud and on-premise appliance
  - AV, IPS, DLP and Content Analysis
- High performance and scalability
  - Custom –built security processing units for high performance
  - Scalability from small to large organizations
  - HA availability for redundancy
- Content Caching and WAN Optimization
  - Static and dynamic content caching
  - Multiple Content Delivery Network
  - Decrease Network Latency
  - Lower bandwidth overhead

Features

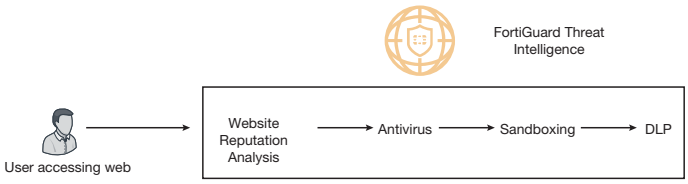
Multi-layered Detection

FortiProxy provides multiple detection methods such as reputation lookup, signature-based detection and sandboxing to protect against known malware, emerging threats and zero-day malware.

Integration with FortiGuard Threat Intelligence

The threat landscape is rapidly evolving, requiring security teams to be continuously vigilant of new threats. FortiGuard Threat Intelligence service is a collection of services delivered by FortiGuard Labs to defend against the changing threat landscape. FortiGuard Labs comprises of more than 200 researchers across 31 countries. It offers 15 different security services and constantly discovers new threats. The following protection services offered by FortiProxy are continuously updated with the latest information from FortiGuard Threat Intelligence.

- **DNS and Web Filtering**
  With the help of FortiGuard Threat Intelligence service, malicious, suspicious and newly generated domain names are blocked immediately. More than 150,000 websites are blocked per minute by the FortiGuard WebFiltering Service. Dynamic category-based web filtering ensure employees abide by the company's acceptable use policy. Static whitelisting and blacklisting capabilities are also available to allow or block specific websites.
- **Dynamic Analysis using Sandboxing**
  Top-rated FortiSandbox is integrated with FortiProxy to defend against targeted advanced attacks. Suspicious and at-risk files can automatically be sent to FortiSandbox for further analysis. The sample is analyzed in a contained environment to uncover the full attack lifecycle using system activity and call back detection. Reports provide rich threat intelligence and actionable insight for security teams to take action.
- **Antivirus and DLP**
  Fortinet consistently receives superior effectiveness results in industry testing with AV Comparatives and Virus Bulletin. Data Loss Prevention protects against exfiltration of sensitive data. Sensitive files can be fingerprinted or watermarked and the outgoing traffic is examined to identify any data leakage.
- **Content Analysis Service**
  FortiProxy includes content scanning technologies from Image Analyzer™, the industry leader in offensive image and video detection to prevent access to inappropriate content.
- **Intrusion Prevention**
  FortiProxy uses a combination of signature as well as signature-less engines to prevent intrusions. IPS signatures can be based on exploits, known vulnerabilities or anomaly patterns. Signature-less techniques are used to detect SQL injection, domain generation algorithm attacks, java and flash exploits. FortiGuard Labs generates more than 100 IPS rules every week, blocking more than 4 million network intrusion attempts.



Inspection of Encrypted Traffic

More than 60% of the internet traffic is encrypted and visibility is a big challenge. FortiProxy offers SSL and SSH deep inspection without requiring any additional license or appliance. It can be used to inspect encrypted traffic by acting as a man in the middle. It also has the flexibility to add exclusion categories so that banking, healthcare and other such sites won't be monitored. When SSL Deep inspection is not possible it also supports Certificate based inspection.

Granular Application Control

With the constant increase in the usage of social apps, it's vital for organizations to provide very granular controls. For instance, they may want to allow access but prevent specific actions like posts. FortiProxy supports all major social websites (including Facebook, LinkedIn, Twitter, Instagram), and supports more than 3000 apps. In addition, SaaS Apps can be classified using the cloud database that's maintained by FortiGuard.

Authenticated Web Access

FortiProxy supports advanced authentication methods including SAML, Kerberos and Single Sign-on. These features are built-in without requiring a separate appliance. It also gives administrators the flexibility to configure policies based on users and roles.

WAN Optimization and Advanced Caching

Today at many locations, bandwidth is a bottleneck, and to keep operation costs low, it may be prohibitive to provide additional bandwidth. In these environments, FortiProxy is also able to greatly optimize and accelerate the network by enabling caching of content and by enabling WAN Optimization features.

Features

Security Fabric

The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises. It can automatically synchronize security resources to enforce policies, coordinate automated responses to threats detected anywhere in your network, and easily manage different security solutions and products through a single console. FortiProxy integrates with key security fabric components such as FortiSandbox and FortiAnalyzer. It can also integrate with third-party security devices using ICAP and WCCP protocols.

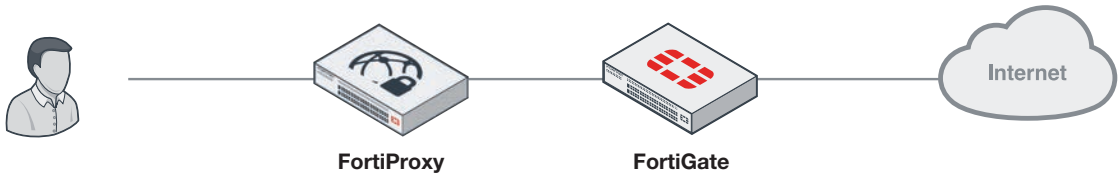
High Performance, scalability and low TCO

FortiProxy uses specialized ASICs in order to accelerate performance of the network and security modules. FortiProxy supports proxy speeds up to 15 Gbps, and can scale from small enterprises with 500 users all the way to larger enterprises of 50,000 users. FortiProxy provides great value to customers while maintaining a low total cost of ownership.

Deployment

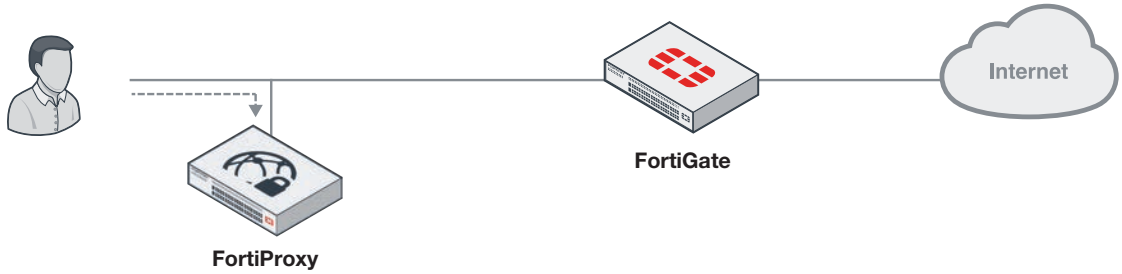
FortiProxy allows you to choose from 3 modes of deployment to meet your specific requirements, while reducing infrastructure changes and service disruptions:

Inline Deployment



- Suitable for smaller enterprises
- Deployed behind the NGFW
- Interesting traffic that needs to be inspected configured on Proxy, and the remaining traffic is automatically bypassed to the NGFW.

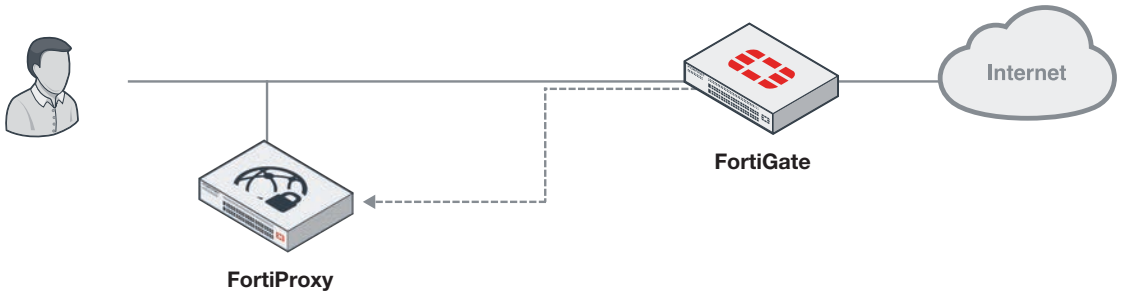
Explicit Deployment



- Suitable for larger enterprises
- Proxy can be deployed in any location within the enterprise
- Support for multiple pac files allows flexibility

Deployment

WCCP/PBR Deployment



- Suitable for larger deployments
- If distribution of pac files is not convenient, WCCP or PBR mode is supported
- Policies are configured on the NGFW/router to direct the interesting traffic to the proxy

Features Summary

System

- Wide range of deployment options:
  – Inline, Forward Proxy, Explicit proxy, WCCP/PBR
  – Hardware or virtual appliance
- IPv4 and IPv6 address support
- Application Support including HTTP/S
- HA available as active-active and active-backup with session synchronization

Threat Protection

- Integration with FortiGuard threat intelligence services for real-time threat updates
- Integration with cloud sandbox to detect advanced threats
- In-built security services requiring no additional appliance
- DNS and Web-Filtering
  – Dynamic categorization of websites
  – Blocking of malicious and suspicious domains and URLs
  – Static blacklists and whitelists
- Application Control
  – Granular web application control for social websites
  – Support for 3000+ applications
- Antivirus, bonet and DLP
- Content Analysis
- Multiple ICAP servers support
- IPS signature & filters
- Web Rating Override
- SSL/SSH Inspection
- Custom Application Signature

Authentication

- Support for various authentication modes including Radius, SAML, LDAP, NTLM, Kerberos, FortiToken One-Time Password
- In-built authentication requiring no additional device

Advanced Caching

- Web and video caching
- Reverse web cache
- Traffic Shaping and QoS policies to prioritize Apps
- Dynamic adaptive streaming over HTTP
- Dynamic adaptive streaming over RTP and RTMPT

WAN Optimization

- Protocol Optimization – support HTTP, MAPI, CIFS, FTP and TCP
- Secure tunneling over across WAN
- Wan Optimization peers

Management and Reporting

- FortiView Integration
- FortiAnalyzer Integration
- Support Syslog server
- Granular role based access
- Reporting and Logging
- Policy tests for ease of deployment

Deployment

	FORTIPROXY 400E	FORTIPROXY 2000E	FORTIPROXY 4000E
System Information			
License Capacity	500–4,000 users	2,500–15,000 users	10,000–50,000 users
Deployment Modes	Inline Proxy, Transparent/WCCP Proxy, Explicit Proxy, Routed Proxy		
Hardware Specifications			
Memory	8 GB	64 GB	128 GB
Management	HTTP/S, SSH, CLI, SNMP, Console RJ45	HTTP/S, SSH, CLI, SNMP, Console DB9	HTTP/S, SSH, CLI, SNMP, Console DB9
Network Interfaces	4x GE RJ45	2x 10 GE SFP+, 2x GE SFP ports, 2x GE RJ45 ports	4x 10 GE SFP+, 2x GE SFP ports, 4x GE RJ45 ports
Bypass Interfaces	—	2x GE RJ45 ports	2x GE RJ45 ports
Storage	4 TB (2 TB x2) Hard Disk	8 TB (2 TB x4) Hard Disk	8 TB (2 TB x4) Hard Disk
Power Supply	Single (Optional Dual)	Dual	Dual
Environment			
Form Factor	1U Appliance	2U Appliance	2U Appliance
Input Voltage	100–240V, AC 60–50 Hz	100–240V, AC 50–60 Hz	100–240V, AC 50–60 Hz
Power Consumption (Average / Maximum)	120 W / 151 W	244 W / 265 W	462 W / 493 W
Maximum Current	100V/5A, 240V/3A	100V/10A, 240V/3.5A	100V/9.8A, 240V/5A
Heat Dissipation	550 BTU/h	940 BTU/h	1,717 BTU/h
Operating Temperature	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-13–158°F (-25–70°C)	-40–158°F (-40–70°C)	-40–158°F (-40–70°C)
Humidity	5–95% non-condensing	8–90% non-condensing	8–90% non-condensing
Dimensions			
Height x Width x Length (inches)	1.73 x 17.24 x 16.38	3.5 x 17.2 x 25.5	3.5 x 17.2 x 25.5
Height x Width x Length (mm)	44 x 438 x 416	89 x 437 x 647	89 x 437 x 647
Weight	25 lbs (11 kg)	32 lbs (14.5 kg)	43 lbs (19.5 kg)
Compliance			
Safety	FCC, ICES, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB		

FortiProxy400E

FortiProxy 2000E

FortiProxy 4000E

軟體標

VIRTUAL APPLIANCE	FORTIPROXY VM01	FORTIPROXY VM02	FORTIPROXY VM04
System Information			
Hypervisor Support	VMware ESX/ESXi, KVM Platform	VMware ESX/ESXi, KVM Platform	VMware ESX/ESXi, KVM Platform
License Capacity	100 users	100–500 users	100–2,500 users
Hardware Specifications			
Storage	2 CPU, Unlimited GB RAM, 1 Disk	4 CPU, Unlimited GB RAM, 2 Disk	8 CPU, Unlimited GB RAM, 2 Disk
Network Interface Support (Maximum)	10	10	10
Management	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP

VIRTUAL APPLIANCE	FORTIPROXY VM08	FORTIPROXY VM16	FORTIPROXY VMUL
System Information			
Hypervisor Support	VMware ESX/ESXi, KVM Platform	VMware ESX/ESXi, KVM Platform	VMware ESX/ESXi, KVM Platform
License Capacity	100–10,000 users	100–25,000 users	100–50,000 users
Hardware Specifications			
Storage	16 CPU, Unlimited GB RAM, 4 Disk	32 CPU, Unlimited GB RAM, 8 Disk	Unlimited CPU, Unlimited GB RAM, 16 Disk
Network Interface Support (Maximum)	10	10	10
Management	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP

Order Information

Product	SKU	Description
FortiProxy 400E	FPX-400E	FortiProxy 400E, 4x GE RJ45 (from 500 users up to 4,000 users).
FortiProxy 2000E	FPX-2000E	FortiProxy 2000E, 2x RJ45 GE, 2x RJ45 GE Bypass, 2x SFP GE, 2x SFP+ 10 GE (from 2,500 users up to 15,000 users).
FortiProxy 4000E	FPX-4000E	FortiProxy 4000E, 4x 10/100/1000 RJ45 Ports, 2x 10/100/1000 RJ45 Bypass Ports, 2x GE SFP Ports, 4x 10 GE SFP+ Ports (from 10,000 users up to 50,000 users).
FortiProxy 400E FortiProxy 2000E FortiProxy 4000E	FC-10-XY400-620-02-DD FC-10-XY2KE-620-02-DD FC-10-XY4KE-620-02-DD	SWG Protection Bundle [Web Filtering, DNS Filtering, Application Control, DLP, AV, Botnet (IP/Domain), Sandbox Cloud] 500 User license with SWG Protection.
FortiProxy 400E FortiProxy 2000E FortiProxy 4000E	FC-10-XY400-160-02-DD FC-10-XY2KE-160-02-DD FC-10-XY4KE-160-02-DD	500 User license with Content Analysis Service.
FortiProxy-VM01	LIC-FPRXY-VM01	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 2x vCPU core, unlimited GB RAM, and 1 TB Disk.
FortiProxy-VM02	LIC-FPRXY-VM02	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 4x vCPU core, unlimited GB RAM, and 2 TB Disk.
FortiProxy-VM04	LIC-FPRXY-VM04	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 8x vCPU core, unlimited GB RAM, and 4 TB Disk.
FortiProxy-VM08	LIC-FPRXY-VM08	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 16x vCPU core, unlimited GB RAM, and 8 TB Disk.
FortiProxy-VM16	LIC-FPRXY-VM16	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 32x vCPU core, unlimited GB RAM, and 8 TB Disk.
FortiProxy-VMUL	LIC-FPRXY-VMUL	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. Unlimited vCPU and RAM support.
Optional Accessory		
Power Supply	SP-FAD700-PS	AC power supply for FPX-400E.

FORTINET

Fortinet Product Matrix

產品	效能	Description	作業版本
Fortinet 標準版資安防護系統 一年授權	防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）及 無線網路控制器（Wireless Controller）	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 標準版資安防護系統 防護升級模組 一年授權	防護升級模組 一年授權		
Fortinet 高階版資安防護系統 一年授權	高階版防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）， 無線網路控制器（Wireless Controller），入侵防禦，應用程式控管，防毒，不當網頁過濾，防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 高階版資安防護系統 防護升級模組 一年授權	高階版資安防護系統 防護升級模組 一年授權		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理，設定和集中派送（政策，資安防禦資料庫）的中央管理系統 r, 支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASEFortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測，提供虛擬的運行環境來分析高風險或可疑的程式，研判威脅完整的生命周期，協助用戶智慧地立即偵測出既存與新興的 網路威脅。	VMware
FWB-Base Fortinet 網站應用程式防火牆(WAF) 25Mbps	網站應用程式防火牆(WAF) 25Mbps	提供網站應用程式防火牆功能（WAF）， 網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式防火牆(WAF) 頻寬升級 100Mbps		

FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡，全球服務負載平衡（GSLB）及線路負載平衡（LLB）等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡 400Mbps	網路負載平衡系統(WAN) 400Mbps	提供網路線路負載平衡，整合不同 ISP 的線路同時並存，提供進出 Internet 的資料流量	VMware ESXi / ESX 5.5, 6.0
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡頻寬升級 400Mbps	網路負載平衡頻寬升級(WAN) 400Mbps		
FC-10-FWV02-851-02-12 Fortinet 網路線路負載平衡 一年續約授權	網路負載平衡系統(WAN) 一年續約授權		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡系統(SLB) (授權方式：依照 CPU 數量 2/4 二個授權方式出貨)	網路負載平衡系統(WAN) 支援 2 CPU		
FSM-AIO-BASE Fortinet 稽核管理系統 50 台設備一年授權	稽核管理系統 50 台設備一年授權	SIEM 應用解決方案，提供收集和整合各種網路和安全資訊，匯整之後進行統一分析和統計，藉以收集、監視和報告企業中的網路設備和資安產品發生的行為，持續進行企業內全面的安全風險評估。	Vmware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure
FSM-AIO-100-UG Fortinet 稽核管理系統升級 100 台設備一年授權	稽核管理系統升級 100 台設備一年授權		
FSM-WIN-ADV-50-UG Fortinet 稽核管理系統 Windows Agent 50 台設備一年授權	稽核管理系統 Windows Agent 50 台設備一年授權		

FC1-15-EMS01-158-02-12 Fortinet 端點(End Point)資安防護 200 Clients 一年授權	端點(End Point)資安防護 200 Clients 一年授權	提供防病毒與惡意軟體檢測、雙因子認證、VPN 等功能，強化企業資安建置。FortiClient 主動防禦高級攻擊。它與 Security Fabric 的緊密集成使基於策略的自動化能夠控制威脅並控制爆發。FortiClient 與 Fabric-Ready 合作夥伴兼容，進一步加強企業的安全態勢。	Microsoft Windows, Windows Server
Fortinet 物聯網安全管理系統 100 台終端設備 一年授權	物聯網安全管理系統 100 台終端設備 一年授權	提供物聯網上每個終端設備的詳細分析以增強其可視性，控管設備之物聯網存取以保障資訊安全，並具備資料分析與報表功能。	VMware, Hyper-V
Fortinet 物聯網安全管理系統升級 100 台終端設備 一年授權	物聯網安全管理系統升級 100 台終端設備 一年授權		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統使用者數量升級 300 人	反垃圾郵件及郵件保全系統使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統(授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UGFortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		
FortiEDR Fortinet 端點偵測、保護與回應系統(雲端版)	Fortinet 端點偵測、保護與回應系統(雲端版)	FortiEDR 提供即時，自動化的端點保護 通信設備-包括工作站和所有伺服器 OT 系統-全部集中集成平台 具有靈活部署和一個可節省的運營成本	無
FortiEDR Fortinet 端點偵測、保護與回應系統(雲端版) 擴充 25 個端點資產	Fortinet 端點偵測、保護與回應系統(雲端版) 擴充 25 個端點資產		
FortiEDR Fortinet 端點偵測、保護與回應系統(本地自建版)	Fortinet 端點偵測、保護與回應系統(本地自建版)		*Windows (both 32-bit and 64-bit versions) XP SP2/SP3, 7, 8, 8.1 and 10 * Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 and 2019 * macOS Versions: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) and Catalina (10.15) * Linux Versions: RedHat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7 and Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 and 18.04.2 server, 64-bit *Virtual Desktop Infrastructure (VDI) environments in VMware and Citrix. VDI Environments: VMware Horizons 6 and 7, and Citrix，XenDesktop 7"
FortiEDR Fortinet 端點偵測、保護與回應系統(本地自建版) 擴充 25 個端點資產	Fortinet 端點偵測、保護與回應系統(本地自建版) 擴充 25 個端點資產		

FortiProxy Fortinet 上網行為控管系統 1CPU (依照 CPU 數量授權方式出貨)	Fortinet 上網行為控管系統 防護升級模組	FortiProxy 是一種安全的 Web 代理，可保護員工免受互聯網傳播的攻擊，結合了多種檢測技術， 例如：如網絡過濾，DNS 過濾，防止數據丟失，防病毒，入侵防禦和高級威脅保護	VMware ESX/ESXi, KVM Platform
FortiProxy Fortinet 上網行為控管系統 防護升級模組	Fortinet 上網行為控管系統 防護升級模組		