# Cisco ASA 5500 系列多功能安全閘道器概述

## Cisco ASA 5500系列總覽

Cisco ASA 5500 系列安全設備為SOHO(小型辦公室/住家辦公室)、中小型企業和大型企業，提供新一代安全和VPN服務的模組化平臺。

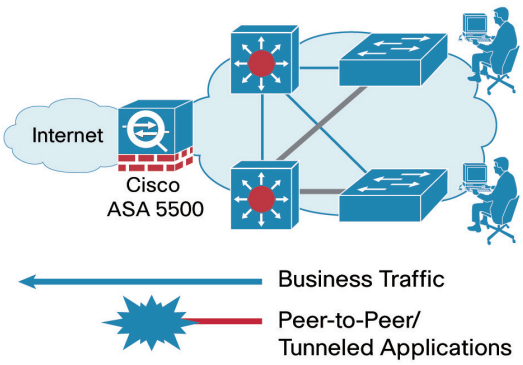
Cisco ASA 5500系列透過四個特別設計的產品版本：防火牆、IPS、Anti-X和VPN版本，完善的支援企業對不同安全功能的特定需求。這些不同版本展現了優異的保護功能，為不同的地點提供了適合該地的服務。每個版本都由多種Cisco ASA服務所組成，提供該版本所專注的功能，以符合企業網路中的不同特殊環境之需求。藉由符合不同網路區段的安全要求，整體網路安全之完整性得以提昇。


Cisco ASA 5500系列在單一平臺上實現了標準化，可降低整體安全營運之成本。簡單一致的設定環境簡化了管理難度、降低員工培訓成本，而此系列單一的硬體平台也大幅降低了維修備品成本。

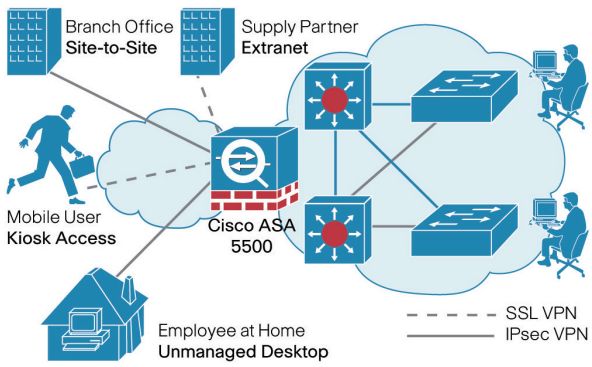
每個版本都可滿足特定企業環境之安全需求：

- **防火牆版本**：使企業能安全、放心地部署關鍵性應用與網路，並透過獨特的模組化設計以提供出色的投資保障和更低的營運成本。
- **IPS版本**：透過結合防火牆、應用層安全功能和入侵防護系統，保護重要商務伺服器和基礎設施免於蠕蟲、駭客和其他威脅的攻擊。
- **Anti-X版本**：以全面的安全服務來保護小型或遠端的用戶，以具備大型企業等級的防火牆和VPN服務，提供安全連線至公司總部。Trend Micro領先業界的Anti-X服務可保護客戶端系統不受病毒、間諜程式、網路釣魚、垃圾郵件和惡意網站威脅。
- **VPN版本**：使遠端用戶可安全存取內部網路系統和服務，支援VPN叢集功能以符合大型企業的環境。此解決方案同時結合了SSL VPN和IPSec VPN遠端登入技術，以及Cisco安全桌面(Cisco Secure Desktop)、防火牆和入侵防護系統等威脅防禦技術，以確保VPN流量不會對企業造成威脅。

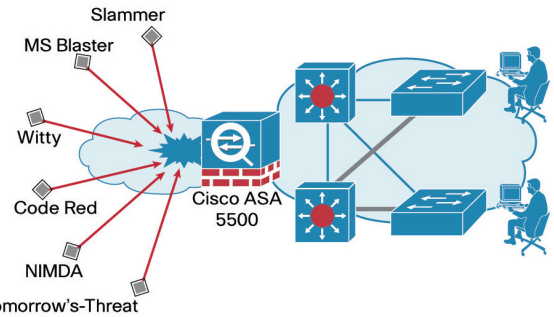
**Market-Leading Application Security**




**Threat-Protected IPsec and SSL VPN Services**




**Industry-Leading IPS/Anti-X Services**




## 五大購買Cisco ASA 5500系列安全設備之理由

**最值得信賴的防火牆技術與VPN威脅防禦技術**

構建於Cisco PIX® 安全設備與Cisco VPN 3000集中器系列的技術。Cisco ASA 5500系列是第一個提供以領先業界的防火牆技術同時保護SSL VPN與IPsec VPN的服務。

**領導市場的Anti-X功能**

在Cisco ASA 5500系列中，結合Trend Micro在威脅防護與內容安全監控領域上的專業技術與Cisco經過市場考驗的成熟安全解決方案，提供了一個全面性的防毒、反間諜程式、檔案阻擋、垃圾郵件、反網路釣魚、URL網站過濾與內容過濾安全方案。

# Cisco ASA 5500 系列多功能安全閘道器概述

### 先進的入侵防禦保護

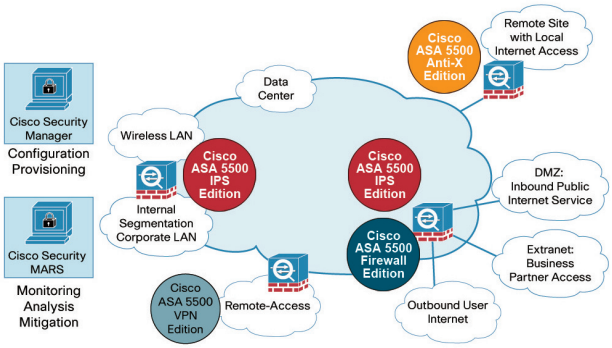
提供具預防功能的完整入侵防護系統以阻擋大規模的威脅，包含病毒、應用程式層級與作業系統層級的攻擊、後門程式、間諜程式、peer-to-peer檔案分享以及即時訊息(IM)。

### 完備的管理與監控服務

藉由內建的Cisco Adaptive Security Device Manager(ASDM)提供直覺式圖形化、單一設備的管理與監控服務，並透過Cisco Security Manager提供企業等級之多元、多台設備管理服務。

### 降低建置與維運成本

藉由提供與現有的Cisco安全解決方案一致的設計與介面，Cisco ASA 5500系列能大幅降低最初的安全設備建置成本與後續每日的管理使用成本。




| Cisco ASA 5500 Series Model/License | Cisco ASA 5505 Base/Security Plus | Cisco ASA 5510 Base/ Security Plus | Cisco ASA 5520 | Cisco ASA 5540 | Cisco ASA 5550 |
|---|---|---|---|---|---|
| Cisco ASA Software Version (latest) | 8.1 | 8.1 | 8.1 | 8.1 | 8.1 |
| Market | SOHO/ROBO/ MSSP/ Enterprise Teleworker | SMB and Small Enterprise | Small Enterprise | Medium-Sized Enterprise | Large Enterprise |
| Performance Summary | | | | | |
| Maximum firewall throughput (Mbps) | 150 | 300 | 450 | 650 | 1200 |
| Maximum 3DES/AES VPN throughput (Mbps) | 100 | 170 | 225 | 325 | 425 |
| Maximum site-to-site and remote-access VPN user sessions | 10 / 25 | 250 | 750 | 5000 | 5000 |
| Maximum SSL VPN user sessions1 | 25 | 250 | 750 | 2500 | 5000 |
| Maximum connections | 10,000 / 25,000 | 50,000 / 130,000 | 280,000 | 400,000 | 650,000 |
| Maximum connections/second | 3000 | 6000 | 9000 | 20,000 | 28,000 |
| Technical Summary | | | | | |
| Memory (MB) | 256 | 256 | 512 | 1024 | 4096 |
| System flash (MB) | 64 | 64 | 64 | 64 | 64 |
| Integrated ports | 8 port 10/100 switch with 2 Power over Ethernet ports | 3-10/100, 1-10/100 OOB2 / 5-10/100 | 4-10/100/1000, 1-10/100 | 4-10/100/1000, 1-10/100 | 8-10/100/1000, 1-10/100 |
| Maximum virtual interfaces (VLANs) | 3 (trunking disabled) / 3 (trunking enabled) | 10 / 25 | 100 | 200 | 200 |
| SSC/SSM expansion slot | Yes (SSC) | Yes (SSM) | Yes (SSM) | Yes (SSM) | No |
| SSC/SSM Capabilities | | | | | |
| SSC/SSMs supported | Future, SSC | CSC-SSM, AIP-SSM, 4GE-SSM | CSC-SSM, AIP-SSM, 4GE-SSM | CSC-SSM, AIP-SSM, 4GE-SSM | No |
| Intrusion prevention | Not available | Yes (with AIP-SSM) | Yes (with AIP-SSM) | Yes (with AIP-SSM) | No |
| Concurrent threat mitigation throughput (Mbps) (firewall + IPS services) | Not available | 150 (with AIP- SSM-10) 300 (with AIP-SSM-20) | 225 (with AIP-SSM-10) 375 (with AIP-SSM-20) | 450 (with AIP-SSM-20) | Not available |
| Anti-X (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering) | Not available | Yes (with CSC-SM) | Yes (with CSC-SM) | Yes (with CSC-SM) | Not available |
| Maximum number of users for antivirus, anti-spyware, file blocking (CSC-SSM only) | Not available | 500 (CSC-SSM-10) 1000 (CSC-SM-20) | 500 (CSC-SSM-10) 1000 (CSC-SM-20) | 500 (CSC-SSM-10) 1000 (CSC-SM-20) | Not available |
| CSC SSM Plus License features | Not available | Anti-spam, anti-phishing, URL filtering | Anti-spam, anti-phishing, URL filtering | Anti-spam, anti-phishing, URL filtering | Not available |
| Features | | | | | |
| Application-layer security | Yes | Yes | Yes | Yes | Yes |
| Layer 2 transparent firewalling | Yes | Yes | Yes | Yes | Yes |
| Security contexts (included/maximum)3 | 0/0 | 0/0 / 2/5 | 2/20 | 2/50 | 2/50 |
| GTP/GPRS inspection3 | Not available | Not available | Yes | Yes | Yes |
| High-availability support4 | Not supported / Stateless A/S | Not supported / A/A and A/S | A/A and A/S | A/A and A/S | A/A and A/S |
| VPN clustering and load balancing | Not available | Not available | Yes | Yes | Yes |