



UU1000

250/500/750/1,000人網路認證閘道器

UU1000為19英吋，1U高度的機架式發佈單元，適合中大型的企業使用。UU1000具有硬體的SSL加速晶片，對SSL協定進行加速。

每一台UU1000可支援250、500、750或1,000人同時上線，UU1000最多可以被叢集至10台。UU1000可以「Standalone Mode」、「Transparent Mode」或是「Router Mode」的不同模式部署在企業現有的網路上；遠端使用者經由「Private Access」或是「Direct Access」存取企業內部資源。UU1000支援Web應用、client/server 應用以及檔案共用存取，它同時也具備Site-to-Site連接功能。

系統連接方式及網路模式：

iSTAR™發佈單元同時擁有極具靈活的系統連接方式及網路模式，在任何的網路環境中都可以部署。

系統連接方式

Direct Access

Direct Access連接方式的部署需使用Public IP位址 (或是DNS名稱)，配合第三方的SSL電子憑證，直接經由發佈單元進行應用存取。

Private Access

您如果沒有Public IP位址，或是想要擁有更高的安全性，此時便可以選擇Private Access連接方式。這種連接方式除了發佈單元之外，還需有交換單元的參與。在Private Access的方式之下，多

台發佈單元(site)可以共用同一張SSL電子憑證，不需要分別各自準備多張電子憑證，尤其適合擁有許多分公司/辦事處的企業使用。

網路模式

Standalone Mode

此一模式下，發佈單元可以建置於內部網路中的任何位置，不改變原網路中的任何設備狀態，只需將發佈單元連接到內部網路的任何一個網路介面上即可，設定安裝極為簡便。

Transparent Mode

此模式下，發佈單元被放置於內部網路和防火牆或路由器之間，不需要變更原有路由器或伺服器的任何配置。

Router Mode

此模式下，發佈單元可以建置在防火牆或路由器的位置上。在提供發佈單元功能的同時，也提供了防火牆和路由器功能。

完整的認證方式

認證方式

iSTAR™可與大多數常見的認證方式相容，包括Windows Active Directory、Windows NT Domain、LDAP伺服器、Radius伺服器，以及Ace伺服器，它同時也具備了本機資料庫功能(local database)。iSTAR™能完整地與您現有的安全認證機制整合。

雙因數(Dual-factor)認證

一些對於安全認證有較高要求的企業，僅採用「使用者名稱加密碼」的登錄方式並不能達到他們的需求，此時iSTAR™支援的雙因數認證方式便能滿足其需要。iSTAR™可支持常見的RSA SecurID® token、one-time password。

客戶端憑證認證(Client-side Certificate)

iSTAR™可以根據位於客戶端機器內的數位憑證對使用者進行認證。系統可以更進一步根據數位憑證的屬性對使用者存取進行限制。

多重安全域(Multi-Realm)

多重安全域提供系統多層次的管理機制。系統會根據使用者登錄時所選擇的安全域，將其對應到指定的認證安全域進行認證。

角色及規則(Roles and Rules)

系統可以根據企業的安全策略制定安全規則(Rules)，再根據規則將使用者分類為不同的角色(Roles)，以便對角色賦予不同的許可權。

共用電子憑證

安裝在發佈單元的第三方SSL電子憑證是為了讓客戶端能夠正確的認證發佈單元(site)，通常多個site需要多張電子憑證。而iSTAR™能夠為多個site提供共用一張電子憑證的部署方式：即Private Access。此時電子憑證位於交換單元而非發佈單元。這種方式能為企業節省必須每年支付多張電子憑證的維護費用。

內建CA

可透過內建的CA中心為用戶發放憑證，PKI協議具有更高的安全性，UU1000內置的CA可以提供X.509憑證的用戶認



證和闖道認證。

■ 方便的授權機制

iSTAR™發佈單元能對單一使用者、多個使用者、群組、多個群組、指定的角色、或是持有客戶端憑證的使用者，分別發佈存取應用、檔案夾，甚至是子網的許可權。與IPSec VPN相比，iSTAR™的授權管理流程十分簡單而且易於理解，不會像一般IPSec VPN產品那樣因為複雜而動輒出錯。iSTAR™發佈單元內有預先制定好的常見應用發佈模組，系統管理人員只需要在這些模組當中挑選需要發佈的應用，便可以輕鬆完成授權的工作。當然，系統管理人員還可以選擇訂制功能，根據自己的需求來訂制特定的應用存取授權。

發佈單元能與大多數現有的認證系統整合，這樣便能有效的運用企業已經存在的認證資料庫，無須另行維護一個獨立的資料庫。

除此之外，發佈單元還能夠規定上線客戶端主機的安全設定，及限制使用者進行存取時間段等強制性的安全策略。

主機檢查(Host checker)

發佈單元具備主機檢查策略，它能夠確保上線的客戶端主機安全設定符合企業制定的策略。主機檢查功能能在客戶端主機對特定的應用進行存取之前，檢查該主機的Windows OS的版本，有沒有安裝適當的Service Pack或是Patch，有沒有安裝適當的防毒軟體，以及該特定應用軟體的客戶端Checksum是否正確。在確認該主機符合企業的安全策略後才允許進行存取。

存取時間段策略(Time-based Policy)

發佈單元能夠制定存取時間的策略，讓使用者只能夠在指定的時段(例如在指定的日期、星期、或是月份)對企業資源進行存取，以增強對企業資源的保護。

■ 服務功能

遠端應用服務功能

- 支援Web應用。
- 支援各種的client-server應用，包括Notes、ERP、NetMeeting、SQL Server、CVS等等。
- 支援host access，包括IBM5250/3270、Telnet等等。
- 支援terminal service，包括Citrix ICA、VNC、Microsoft Terminal Services、Windows XP Remote Desktop、Radmin等等。
- 支援電子郵件，包括Outlook、Outlook Express、Notes、Eudora等等。
- 實現對FTP、SMB以及NFS標準的檔案伺服器進行瀏覽、存取及管理的功能。

子網服務功能

UURemote提供遠端使用者使用整個子網路資源的功能，如同直接連接在該子網路上一樣。

而UUsoft適用於將位於遠端的伺服器連接到子網上，它具有「自動連線」(Always-On)的功能。UUsoft的特性讓企業內部的IT管理人員，甚至是外包IT服務公司，可以遠端管理異地的伺服器。

■ Site-to-site服務功能

Site-to-site服務功能提供不同的site之間，除了專線連接之外的另一種更為經濟的连接方式。彼此透過安全通道相互連接在一起，共用彼此的資源。

■ 系統管理功能

本機及遠端管理功能

系統管理人員可以對iSTAR™全系列產品進行本機或是遠端的管理，無論是本機或是遠端管理，其介面(GUI)操作均為一致。而所有管理資訊都經由SSL通道加以保護。

日誌管理

系統提供了6種不同的日誌等級供系統管理員選擇。

警示設定

警示級別的設定由系統管理員來決定，警示資訊可經由電子郵件或指定系統送達指定人員的信箱或是呼叫機。

查看系統功能

經由圖表方式顯示系統資源使用情況，以供管理員查詢。

■ 叢集、負載平衡和高可靠性

您可以根據實際的需要逐步地擴充iSTAR™系統，UU1000發佈單元以及交換單元均可以被叢集至10台，負載平衡技術為叢集的設備彼此間提供備援保護機制，提高了系統的可靠度。

叢集(Clustering)

iSTAR™系統採用叢集技術，無論是多台發佈單元或是交換單元，均可以經由叢集構建大容量的系統。所有叢集在一起的單元就如同一個單一的系統，只需設定其中某一台設備，其餘的設備會經由叢集獲得相應的配置。

負載平衡(Load balancing)

經由負載平衡技術，流量均勻的被分佈在多台叢集的設備上，您可以根據同時上線人數的增加逐步地擴充系統。

N+1高可靠性(High availability)

在一個叢集中如果某一台設備出現故障，將會減少相對應的同時上線人數數量。為了保證同時上線人數不因為單一的設備故障而受到影響，您可以選擇在叢集中多加一台設備作為容量備援。在叢集N台設備之中再加入一台設備，形成N+1的高可靠性保護機制，是十分經濟的解決方式。

電源	輸入	AC90~264V @ 47~63Hz
	輸出	250W
外觀	尺寸	426 x 44 x 350mm (16.7" x 1.7" x 13.7")
	重量	~4.5Kg (~9.9lb)
環境要求	溫度	0~40°C (32~104°F)
	濕度	5~85%@40°C (104°F)
網路介面	4個10/100/1000 Base-TX	

群浩科技股份有限公司

110台北市信義區忠孝東路五段508號7F之1 TEL: 02-2727-8080 FAX: 02-2727-5544
7F-1, No.508, Sec. 5, Zhongxiao E. Rd., Xinyi Dist., Taipei City 110, Taiwan (R.O.C.) TEL: +886-2-2727-8080 TEL: +886-2-2727-5544