

# 大型企業整合運用 應用範例

你  
·  
簡  
單  
用  
網  
路  
·  
複  
雜  
問  
題  
我  
們  
處  
理  
!

## ■ 側錄即時通訊、WEB、FTP、WEB，該用什麼設備？

### 描述

對於網路通訊而言，『記錄』這個字眼有很多意義，它可以是下列4個的一種或是全部，但是不論哪一個，ShareTech的UR系列都能滿足你的需求。

#### 1、管理介面登入紀錄：哪一個管理者，何時，從哪裡(IP位址)登入，做了哪些事？

一部UTM可能多個管理者，而管理者可能來自四面八方，紀錄誰從哪邊來，在何時做了哪些事情，是一部UTM基本的要求，ShareTech 甚至管理者將改變前跟改變後的內容一併紀錄下來，同時並列出，讓人容易的比較。

#### 2、系統服務的紀錄：病毒引擎何時更新病毒碼，更新是否成功。PPTP 用戶何時登入，用了多久？

這些服務事關整個UTM能不能運作正常的關鍵，這些訊息都被紀錄下來，讓管理者知道，問題是從哪時候開始的。

#### 3、網路封包通聯記錄：每一個封包何時出去，用哪個PORT出去，目的 IP位址是哪裡，目的PORT是多少？

不論是要查詢網路攻擊者或是被攻擊者，網路服務是否正常，藉由封包的通聯記錄可以知道實際的問題點是在哪裡。

#### 4、流量分析記錄：今天哪一個 IP 位址網路流量(TOP 50)最大？ 這個最大使用量的人他用哪一個協定最多是WEB還是 MAIL，佔用的比例是多少？

#### 5、通訊內容記錄：使用者到過哪幾個網站，瀏覽過哪些網頁，傳送、接收的信件內容是甚麼？用 FTP 上傳下載哪些資料，將這些資料備份，以備不時之需。



## 大型企業整合運用 應用範例

你  
·  
簡  
單  
用  
網  
路  
·  
複  
雜  
問  
題  
我  
們  
處  
理  
!

目前支援的功能有 WWW、MAIL(SMTP 跟 POP3)、FTP、MSN、Yahoo、ICQ、IRC、Gadu、Jabber等。

除了統計分析的資料外，ShareTech UTM(UR系列)更能提供內部每一個IP位址的即時流量跟連線數量，有經驗的管理者可以藉由這項資料，判斷哪一部電腦正在不當地使用網路，再藉由管制條例的運用，立刻管制。