UR-918 UTM 記錄器

ShareTech

網路在追求速度之外，還是必須要能兼顧安全，才可以幫企業打造一個穩定的工作環境。眾至 UR-918 多功能防火牆就是一台兼具速度與安全的設備，除了具有防火牆 (Firewall) 功能外，還擁有防毒、防垃圾、內容記錄 (郵件、即時通訊、IM.) 、IDP 入侵偵測、BOTNET 防禦、頻寬管控、自定義 port、異常 IP 分析、協同防禦、上網行為管理、ARP 防偽、交換器 (Switch) 協同管理、負載平衡、內容過濾、CMS 中央控管、虛擬私有通道 (IPSec VPN) 等多項強大功能。UR-918 適合不同規模的中、小型企業及辦公室網路環境運用，一次滿足中小企業對於網路安全防禦的需求。協助中小企業在網路閘道第一線即時攔截各式病毒威脅同時，仍讓網路保有令人驚豔的優異效能。

(一) 功能特色

防火牆

UR-918 內建 SPI 技術，主動攔截、阻擋駭客攻擊，不論是 SYN、ICMP、UDP 等攻擊方式都可以阻擋。眾至資訊主要是套用合理流量的觀念，認為每個來源不會同時產生太多封包，萬一超過設定的合理封包數時，防火牆會要求將多餘的封包阻擋。

IP V4 / V6 雙頻技術

UR-918 除了支援以往 IPV4 網路環境外，亦支援最新的 IPV6 網路協定，可以提供企業 IPV4 與 IPV6 並行的網路架構。同一個網路介面，不管它被定義成 WAN 或是 LAN，都可以同時綁定 V4 或 V6 的 IP 位址，所以不管是在純 V4 的環境、V4/V6 混合、純 V6 的環境，UR-918 都一樣合用。

病毒信過濾

Clam AV 防毒引擎防護，系統免費提供 Clam AV 防毒引擎，可偵測 800,000 種以上的病毒、蠕蟲、木馬程式，不論電子郵件、WEB、FTP 通通會自動掃描病毒，每日自動透過網際網路更新病毒檔，並提供病毒郵件排行榜報告。

Web、FTP 反病毒過濾服務

當使用者開啟瀏覽器存取某網頁時，UR-918 會依系統所設定判別網頁的安全性，並可針對檔案的上傳、下載做過濾及檔案阻擋規則。根據以往經驗，利用 FTP 下載資料最容易讓自己的電腦中毒。所以利用網路做下載與上傳檔案須特別注意，因為有可能一不小心就讓自己的資料毀於一旦。UR-918 防毒牆幫企業做好 FTP 上傳掃描與下載掃描的服務，並且可以阻止員工利用 FTP 下載檔案，為企業網路安全做好安全服務。

垃圾信過濾

內部郵件或外部郵件都可以過濾，並提供 ST-IP 網路信評、快速 ST-PIC 多維圖形辨識技術、貝氏過濾法、貝氏過濾法自動學習機制、 灰名單、自動白名單機制、垃圾信特徵過濾與指紋辨識法等，並有黑、白名單比對和智慧型辨識學習資料庫（Auto-Learning），甚至可以設定個人化規則，彈性制定過濾規則，處理垃圾郵件，無誤判確保全面性防護，準確率達 95%以上。郵件過濾，能將符合管理者設定過濾條件的信件，執行轉送、刪除、阻擋等動作。

IDP 入侵防禦

IDP 它會檢查對應到 OSI 模型第 4 到 7 層的內容，是否有惡意的攻擊程式、病毒，隱藏在 TCP/IP 的通信協定中，透過詳細的內容檢查後，符合條件的特徵碼就會被標示出來，一旦發現後能夠即時地將封包阻止，讓這些穿過防火牆的惡意封包無所遁形。

完整郵件紀錄

針對所有進出郵件伺服器或郵件閘道器的郵件，連同夾帶檔案，通通記錄下來，最重要的是儲存郵件的格式是 eml，在任何作業系統下都可以輕易的閱讀或搜尋。

詳細記錄 WEB、FTP、MSN、Mail 內容

側錄 WEB、FTP 傳檔、MSN 對話內容及傳檔、IM（Yahoo、ICQ、IRC、Gadu、Jabber）與郵件的傳送接收等內容記錄，隨著管制條例的運用，自動備份特定使用者的所有來往資料。

內網防護(ARP 防偽)

對 UTM 而言，最難偵測到的攻擊類型就是廣播型的封包，如 ARP 欺騙、私架 DHCP 伺服器等，因為通訊協定的先天性缺陷，導致這一類的攻擊行為很難被偵測出來，眾至 UR-918 的 ARP 偵測機制，可以在第一時間內就找到『濫發佈』 ARP 訊息的人。另外，也可搭配協同防禦交換器的設備，可以標示出這個 IP 的實體位置，讓他無所遁形。

異常 IP 分析

任何網路行為，不論使用者執行哪一種軟體，從網路封包的角度，大致分成上傳、下載的連線數量(Connect Seesion)、流量(Flow)跟持續時間(Time)，藉由偵測這些數量的組合，推估使用者是正常使用網路或是有異常的行為。當發現內部使用者異常行為後，管理者可以採取多種策略，例如，阻擋上網、立即限制他的最大頻寬、啟用協同防禦機制通知交換器將他封鎖或是通知管理者就好。

協同防禦(搭配 SNMP 交換器)

協同防禦屬於 UTM 的進階防護，透過異常 IP 分析、交換器（Switch），即時監控內部機器的分部狀況，當內部網路發出大量異常封包時，阻擋這些封包的傳送，並協助管理人員盡速排除異常狀態，可以在事件發生的第一時間內知道哪一個電腦在哪一個交換器 PORT 上，避免企業網路癱瘓。眾至 UR-918 協同防禦機制，不需要改變網路架構，不需要更昂貴的專門 Switch（具備 Layer 2 就可以）、不需要增加任何額外的偵測設備、不用改變每一個使用者的網路習慣，讓網路管理的動作變得簡單、直覺。

BotNet 協同防禦

ShareTech 的 UTM 兼具 BotNet 功能，因為本身兼具 NAT 的功能，當內部的使用者利用郵件伺服器寄出垃圾信件或是直接對外，UTM with BotNet 的偵測設備都可以明確地指出，哪一台才是真正的攻擊來源，也才有辦法將有危害的網路封包直接封鎖。萬一，UTM 的 BotNet 阻擋事件發生後，特定電腦仍然持續的對外攻擊，為確保 UTM 的 CPU 資源不會被浪費在同一件事情上，管理者可以啟用 BotNet 的協同防禦機制，將有問題的電腦 Switch Port 直接關閉，不僅可以節省 UTM 的資源，也確保內部網路不會被這個殭屍病毒持續危害。

IP/MAC/Port 互鎖

在某些敏感度比較高的網路環境，例如軍方、政府單位、研究機構等，不希望使用者任意地更換 Switch 的實體位置，以下面的使用者 A(IP:192.168.100.5，MAC:05:51:62:53:02:03)為範例，透過 UR-918 可以將它定位在 Switch 第 3Port 孔，如果他換到任何 Switch 的不同孔位，設備就會不通。

內容過濾

使用者可自行定義關鍵字阻擋不當的網址，並可阻擋使用者直接使用 IP 位址上網。能阻擋由 Java applets 與 Active X 所控制的自動下載、網站 Cookies 等檔案形式：阻擋工作端存取不當網頁(如色情、暴力)和攻擊性網頁(如駭客、病毒)，且能自設過濾條件，阻擋不當網站。

URL 資料庫管理

UR-918 內建「雲端 URL 資料庫」，自動將網頁分類，管理者只要針對有害的 URL 網進行防堵，可以輕鬆管制，不需要再逐一輸入網站 IP 位址、關鍵字....來阻擋。任意點選有害的 URL 網址是罪惡的淵源，最好的防堵方式是禁止使用網路，如果無法全面禁止，使用時時更新的 URL 資料庫就是最好的防護機制。

負載平衡

UR-918 具有負載平衡的功能，可藉由多條專線及 ISP 之連線服務，改善對外網路連取效能。負載平衡主要可提供當某條專線或某個 ISP 連線出了問題時，可自動切換有問題的線路，轉到其他正常線路繼續服務。UR-918 具有對外/對內負載平衡(Outbound / Inbound balance)，提供自動分配與手動分配等平衡模式供企業選擇。

頻寬管理功能(QOS)

UR-918 可以協助網管人員控管網路流量，有效的減緩企業網路的阻塞、提升服務性與頻寬使用率。具有 QoS(頻寬管理)功能，可將有限的頻寬分給所有使用者。與一般頻寬管理器的差異是，多功能防火牆除了可以提供最大頻寬、優先順序管理之外，還具有保證頻寬功能。並且還具有個人化頻寬管理之設計，可針對個人使用者做頻寬管理之設定。若頻寬管理搭配個人化頻寬管理使用時，可將頻寬管理功能所預留的頻寬，再分配給企業下面之使用者，可有效防範頻寬被使用者獨佔之現象。

應用程式管制

各種網路應用軟體不僅管理不易，更容易成為資料洩密、病毒攻擊的最佳管道。UR-918 內建多種應用程式管理功能，如 P2P 軟體、即時通訊軟體、WEB、娛樂軟體、其他，可輕鬆控管員工使用應用軟體之許可權，保護企業網路安全。

認證 Authentication

提供本機使用者/AD/POP3/Radius 認證授權機制，可協助網管人員與監控企業內部所有使用者帳號，在確認使用者的 ID 的有效授權之後，才能允許其使用網路，讓企業可以有效管理網路使用資源。

VPN 功能

企業員工在外如果想取得公司最新資料，常利用電腦連上開放的網際網路上去截取，但是利用開放性的網際網路來傳輸資料容易被竊取，資料有傳輸安全上的憂慮。因此，多數的企業會在 Server 上設定 VPN，讓使用者從外進行連機時，都必須通過重重的驗證才能進入。VPN 就是在使用者與公司主機間產生一條加密的通道，傳輸重要資料。

- IPSec VPN

  適用在總公司與分公司之間的傳輸，可同時支援多台電腦與遠端伺服器之間的連機。IPsec VPN 適用於需要同時支援多台電腦及伺服器彼此連機，且地點固定的企業環境中，可以得到相當良好的管理及安全保障機制。

- PPTP VPN

  適合固定地點與公司之間的傳輸。例如：員工從家中與公司之間的傳輸。較適合使用在地點固定的公司間連機傳輸

- SSL VPN 連接及管制

  SSL VPN 是一種具有安全加密保護的虛擬私人網路技術，可以讓使用者在外地使用電腦的時候，就像是在區域網路裡面使用電腦一樣，可以使用任何只有在區域網路內才能使用的資源，如 ERP、進銷存或是限定來源 IP 位址的圖書查詢系統，又因為將資料加密，所以在網際網路上無法解析傳輸的內容，確保雙方傳輸資料的安全性。SSL VPN 具備有管制功能，對於遠端用戶而言，管制有 2 個方向，一個是進入內部網路，另一個是透過 VPN Server 上網際網路(可以選擇啟用或是關閉這項功能)，這 2 個管制方向都可以管制遠端用戶使用的頻寬、通訊服務及時間。

CMS 中央管理系統

想要管理分散在各地的 UTM 設備，只能靠網路管理者的頭腦、電腦記憶或是購買昂貴的網管軟體，UR-918 把你需要的遠端設備管理軟體內建，就像一大串的肉粽一樣，抓住頭，就抓住下面所有設備的動靜。不用 DDNS，不用額外的軟體，熟悉的管理介面，一台搞定 N 台。

圖形化流量報表

提供 WEB 介面的流量報表，將系統歷史狀態繪成圖表，讓管理者可以很隨時掌握目前系統運作狀態。目前 UR-918 提供系統狀態圖表(包含 CPU 負載圖、記憶體負載圖、系統負載)、網路流量圖表(LAN 流量、WAN1 流量、WAN2 流量與 DMZ 流量)，並提供查詢條件可以快速搜尋各流量狀態歷史紀錄。

網路測試工具

使用者可由系統主動發送封包（利用 Ping、Traceroute、DNS Query、Server Link 模式），得知目前連外線路的資料傳輸品質和狀態。

靈活管制條例操控

UR-918 具有靈活的管制條例設計，管理人員可用各種排列組合方式達到企業網路管控的需求，所以操作皆在同一個介面中設定，並不需要停止服務即可立即修正，方便網管人員操作維護。

支援一組 Lan Bypass

為預防網路系統當機的問題，除針對電源輸入異常時，也支援 LAN bypass 功能，在機器故障時會自動將網路接線自動導通，確保所有對外的網路保持暢通，也可提昇系統穩定及安全性。

多功能管理介面

使用 Web 方式設定和更新韌體，操作畫面可隨時切換為繁體中文／簡體中文／英文，並具有設定檔匯入、匯出的功能。

(二) 硬體規格

- 網路介面
  2WAN / 1LAN / 1DMZ
- 網路速度
  10/100 /1000Mbps
- 記憶體
  2G
- 硬碟
  SATA 160G
- 系統管理
  使用流覽器進行管理設定
- 安規認證
  FCC、CE
- 使用環境
  作業環境溫度：0℃ ~ 45℃
  作業環境濕度：-20% ~ 70% RH
- 產品尺寸
  44mm (高) ×430mm (寬) ×255mm (深)
- 帳號數目
  無限制
- 適合環境
  中小企業 50~75
- 機型
  1U 機架型
- 電源
  100V~240V / 60W

如有任何需要，歡迎和我們聯絡

鋭吉科技有限公司
Http://www.rayji.com.tw
電話：04-26332215 傳真：04-26332216
E-Mail：service@mail.rayji.com.tw