

# 中華電信數據通信分公司

## HiNet 入侵防護服務報表說明書

# 目 錄

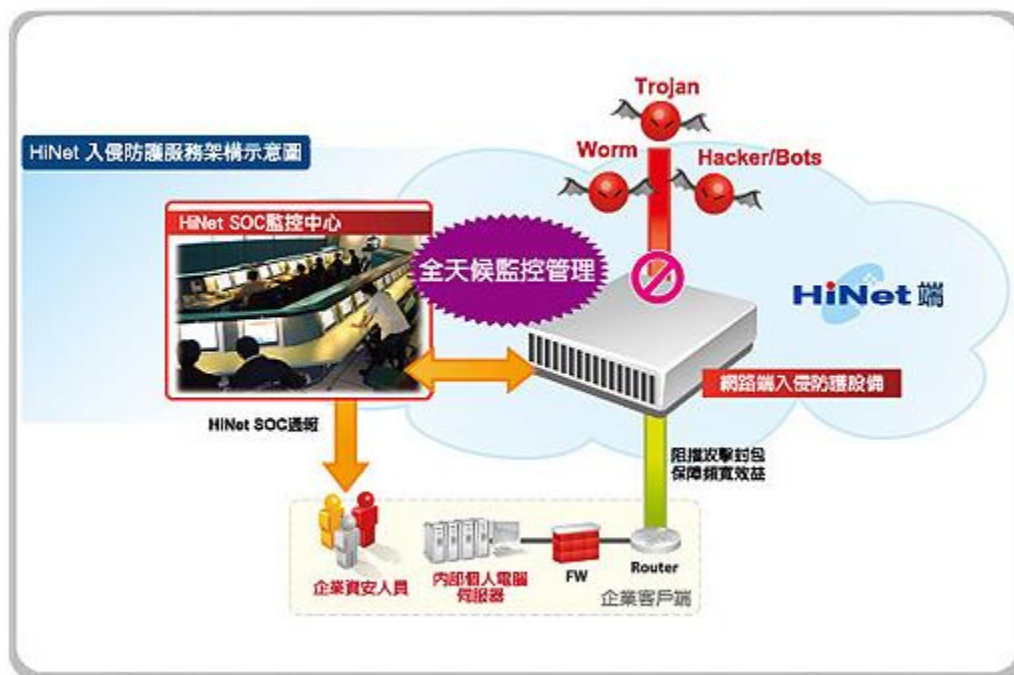
一、	HiNet 入侵防護服務概述.....	1
二、	申請 HiNet 入侵防護服務.....	3
1	如何登入企業資安服務網站.....	3
2	如何納管我的線路 .....	5
三、	如何修改通報聯絡資料.....	9
1	中華電信/HiNet 會員通報信箱查詢與修改.....	9
2	電路資料查詢與修改.....	11
3	全球預警情報發送信箱查詢與修改.....	12
四、	網站總覽.....	13
1	即時監控 .....	13
1.1	總量.....	13
1.2	通訊埠.....	15
1.3	設定.....	16
2	分析摘要 .....	16
2.1	本日摘要.....	16
2.2	本日排名.....	17
3	自訂查詢 .....	18
3.1	查詢.....	18
4	統計報表 .....	22
4.1	日報.....	22
4.2	週報.....	24
4.3	月報.....	26
5	說明.....	28
5.1	攻擊資料庫.....	28
5.2	問答集.....	28



名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

### 一、HiNet 入侵防護服務概述

本手冊之目的，乃是教導已申請「入侵防護服務」服務（以下簡稱本服務）之用戶透過「HiNet 企業資安服務網站」(<http://soc365.hinet.net>) 查詢本服務之統計報表。本服務示意圖如下：



(圖一-1：入侵防護服務示意圖)

本服務統計報表主畫面提供兩層式功能選單，其功能如下表所示：

表一-1：統計報表功能選單

	功能	說明
1. 即時監控 (Monitor)	總量	以圖表顯示過去 24 小時內的攻擊次數時間趨勢。
	通訊埠	以圖表顯示指定通訊埠 (port) 個別的攻擊次數時間趨勢。
	設定	用戶可設定欲監控的通訊埠。
2. 分析摘要 (Analysis)	本日摘要	過去 24 小時內的攻擊摘要。
	本日排名	過去 24 小時內的攻擊統計排名。
3. 自訂查詢 (Query)	查詢	用戶可依自訂條件查詢攻擊的詳細資料。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0
4. 統計報表 (Report)	日報	可觀看每日的攻擊統計報表。	
	週報	可觀看每週的攻擊統計報表。	
	月報	可觀看每月的攻擊統計報表。	
5. 說明 (Help)	攻擊資料庫	可查詢資安攻擊的完整說明。	
	問答集	客戶可能的疑問及回答。	

本服務統計報表畫面如下圖所示：



(圖一-2：入侵防護服務報表畫面)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 二、申請 HiNet 入侵防護服務

### 1 如何登入企業資安服務網站

步驟一：請先連至 HiNet 首頁：<http://www.hinet.net>，並點選畫面中左方選單的「資安/物聯網」－>「入侵防護」選項。

The screenshot shows the HiNet website homepage. On the left sidebar, the menu item '資安/物聯網' (Security/IoT) is highlighted with a red box and labeled '1'. In the main content area, the '企業資安' (Enterprise Security) section is highlighted with a red box and labeled '2'. Within this section, the '入侵防護' (Intrusion Prevention) link is also highlighted with a red box.

(圖二-1-1：HiNet 首頁)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟二：請點選畫面右上方的「會員登入」，以便連結至企業資安服務 VIP 專區。



(圖二-1-2：中華電信入侵防護服務頁面)

步驟三：請先登入中華電信會員中心。（若您已擁有會員中心的帳號，則請跳過以下步驟；若您無會員中心的帳號，則請您點選畫面下方的「加入會員」按鈕，即可免費註冊一組新的中華電信會員中心帳號）



(圖二-1-3：中華電信會員中心登入畫面)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟四：請選擇畫面右方「Email註冊」或「手機註冊」進行註冊。



(圖二-1-4：中華電信新會員註冊選擇頁面)

## 2 如何納管我的線路

步驟一：登入中華電信會員後，請點選左方功能選單中的「群組電路」。



(圖二-2-1：進入「群組我的電路」)



名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟二：請輸入使用 HiNet 入侵防護服務的用戶號碼及密碼（若您不清楚用戶號碼及密碼之使用方式，請點選畫面中「用戶號碼與密碼說明」按鈕），再點選「新增至我的產品」按鈕，即可將線路帳號匯入所屬的中華電信會員中心帳號以便觀看報表。

新增至我的產品成功後，畫面下方「我的產品」欄位將出現您所新增的記錄。



(圖二-2-2：群組我的電路)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟三：請點選左方功能選單中的「下載專區」。

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區**
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改

首頁 > 產品監看中心 > 下載專區

下載專區

項次	方案名稱	HN	公司名稱	資安服務名稱	起租日期	下載
1	HiNet UTM代管服務超值旗艦方案(UTM設備租用+現場安裝維護+防護代管方案)	1007		UTM代管服務	2008-09-01	下載
2	是方IDC入侵防護服務	599		入侵防護服務(施工中)	2011-12-27	下載
3	HiNet入侵防護服務(多機型), 前三個月免收費, 第四個月起每月499元	710	中華電信股份有限公司數據通信分公司	入侵防護服務	2007-03-26	下載
4	HiNet資安艦隊2009方案(內含HiNet UTM代管服務, 需綁約兩年)	710	中華電信股份有限公司數據通信分公司	UTM代管服務	2009-02-17	下載

(圖二-2-3：進入「我的資安服務與下載專區」)

步驟四：您可於畫面下方瀏覽已申請的資安服務，您可點選資安服務類別的服務進入管理介面，例如要進入「入侵防護服務」管理介面，請點選「入侵防護服務」，即可進入管理介面。

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區**
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改

首頁 > 產品監看中心 > 下載專區

下載專區

項次	方案名稱	HN	公司名稱	資安服務名稱	起租日期	下載
1	HiNet UTM代管服務超值旗艦方案(UTM設備租用+現場安裝維護+防護代管方案)	1007		UTM代管服務	2008-09-01	下載
2	是方IDC入侵防護服務	599		入侵防護服務(施工中)	2011-12-27	下載
3	HiNet入侵防護服務(多機型), 前三個月免收費, 第四個月起每月499元	710	中華電信股份有限公司數據通信分公司	<b>入侵防護服務</b>	2007-03-26	下載
4	HiNet資安艦隊2009方案(內含HiNet UTM代管服務, 需綁約兩年)	710	中華電信股份有限公司數據通信分公司	UTM代管服務	2009-02-17	下載

(圖二-2-4：進入各服務管理介面)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟五：請點選「下載」按鈕，即可下載本服務之報表操作說明。

HiNet 企業資安服務

我的產品 | 會員登出 | 我要申租

產品訊息 | 最新消息 | 成功案例 | 媒體報導 | 下載專區 | FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區**
- 全球預警備報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改

首頁 > 產品監看中心 > 下載專區

下載專區

項次	方案名稱	HN	公司名稱	資安服務名稱	起租日期	下載
1	HiNet UTM代管服務超值旗艦方案(UTM設備租用+現場安裝維護+防護代管方案)	1007		UTM代管服務	2008-09-01	下載
2	是方IDC入侵防護服務	599		入侵防護服務(施工中)	2011-12-27	下載
3	HiNet入侵防護服務(多機型)，前三個月免收費，第四個月起每月499元	710	中華電信股份有限公司數據通信分公司	入侵防護服務	2007-03-26	下載
4	HiNet資安應隊2009方案(內含HiNet UTM代管服務，需綁約兩年)	710	中華電信股份有限公司數據通信分公司	UTM代管服務	2009-02-17	下載

(圖二-2-5：各服務報表操作說明與下載)

- 請接續「四、網站總覽」參考入侵防護服務報表網頁介紹。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

### 三、如何修改通報聯絡資料

當用戶租用入侵防護服務之後，系統會提供定期報表寄送及事件通報等服務，客戶可依下列說明查詢或修改接收資安通報的聯絡資料。

#### 1 中華電信/HiNet 會員通報信箱查詢與修改

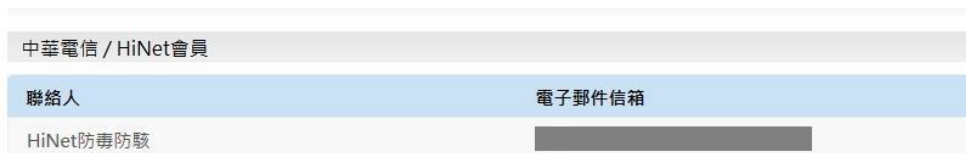
步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請 HiNet 入侵防護服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢中華電信/HiNet 會員聯絡資料請點選左方功能選單中的「通報聯絡資料」。



(圖三-1-1：進入「通報聯絡資料」)

步驟三：畫面中第二項「中華電信/HiNet 會員」的聯絡人資訊，即為入侵防護服務之通報聯絡資訊。



(圖三-1-2：中華電信/HiNet 會員聯絡人資訊)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

步驟四：如欲新增或修改通報聯絡資訊，請先登入中華電信會員中心：<http://member.hinet.net/MemberCenter/index.jsp>，並點選畫面左方選單的「帳號與聯絡資訊設定」。



(圖三-1-3：中華電信會員基本資料修改服務)

步驟五：於「聯絡信箱」項目，點選「立即設定」按鍵，即可修改通報聯絡信箱。



(圖三-1-4：中華電信會員聯絡信箱)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 2 電路資料查詢與修改

步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請 HiNet 網路入侵防護服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢電路資料請點選左方功能選單中的「電路資料修改」。

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區
- 全球預警情報

設定

- 群組電路
- 通聯聯絡資料
- 電路資料修改**

首頁 > 設定 > 電路資料修改

電路資料修改

- ◆ 點選[用戶號碼]：固定IP之服務，用戶可查詢電路的MRTG流量圖。
- ◆ 點選[用戶名稱]：固定IP之服務，用戶可查詢或修改用戶CPE資料。
- ◆ 點選[用戶IP]：固定IP8個月以上之服務，用戶可查詢TWNIC whois database所登記之IP資料。

產品名稱	用戶號碼	用戶名稱	連線速度	使用狀態	用戶IP
	1007		/100M	使用中	203.7
	898		/未知	使用中	
N/A	899	測試產品	/未知	使用中	
	899		/未知	使用中	
	899		/未知	使用中	

(圖三-2-1：進入「電路資料修改」)

步驟三：畫面中點選「用戶名稱」即可查詢或修改電路連絡資料。

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區
- 全球預警情報

設定

- 群組電路
- 通聯聯絡資料
- 電路資料修改**

首頁 > 設定 > 電路資料修改

電路資料修改

- ◆ 點選[用戶號碼]：固定IP之服務，用戶可查詢電路的MRTG流量圖。
- ◆ 點選[用戶名稱]：固定IP之服務，用戶可查詢或修改用戶CPE資料。
- ◆ 點選[用戶IP]：固定IP8個月以上之服務，用戶可查詢TWNIC whois database所登記之IP資料。

產品名稱	用戶號碼	用戶名稱	連線速度	使用狀態	用戶IP
	1007		/100M	使用中	203.7
	898		/未知	使用中	
N/A	899	測試產品	/未知	使用中	
	899		/未知	使用中	
	899		/未知	使用中	

(圖三-2-2：電路資料修改)



名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

### 3 全球預警情報發送信箱查詢與修改

步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請 HiNet 入侵防護服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢全球預警情報發送信箱請點選左方功能選單中的「全球預警情報」。



(圖三-3-1：進入「全球預警情報」)

步驟三：畫面中「發送 E-Mail」即為全球預警情報發送信箱，可勾選或進行修改。



(圖三-3-2：「全球預警情報」畫面)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

#### 四、網站總覽

完成申請入侵防護服務後，即可開啟入侵防護服務報表網頁，網頁提供功能畫面如下圖所示：

The screenshot shows a web interface for intrusion protection reports. At the top, there is a navigation bar with '主功能選單' (Main Function Menu) containing '即時監控 (Monitor)', '分析摘要 (Analysis)', '自訂查詢 (Query)', '統計報表 (Report)', and '說明 (Help)'. Below this is a secondary menu '次功能選單' (Sub-function Menu) with '總覽' (Overview), '通報率' (Reporting Rate), and '設定' (Settings). The main content area, labeled '報表內容' (Report Content), displays a line graph titled '即時監控圖 (過去24小時)' (Real-time Monitoring Graph (Past 24 Hours)). The graph plots the 'Number of Attacks' on the y-axis (0 to 40) against time on the x-axis (15:00 to 15:00 the following day). Below the graph is a table of attack results (評價結果) with columns for '來源IP' (Source IP), '目標IP' (Target IP), '風險' (Risk), '攻擊名稱' (Attack Name), 'Bytes', and '時間' (Time). The table lists several attacks, mostly identified as 'Worm-Welchia\_scmp' with a risk level of 'high' and 0 bytes transferred. One attack is identified as 'MS-SQL-Resolution-Overflow' with a risk level of 'high' and 3 bytes transferred.

(圖四：入侵防護服務報表網頁區塊介紹圖)

以下針對主功能選單選項做個別的說明：

### 1 即時監控

#### 1.1 總量

即時顯示過去 24 小時內的攻擊次數時間趨勢



名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

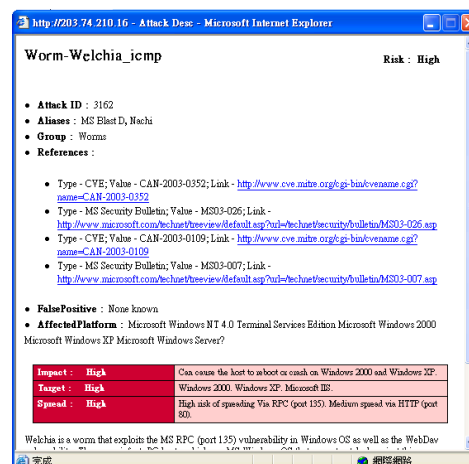


(圖四 1-1：即時查詢-總量)

- (1) 即時監控圖：可看出每小時用戶端在網路上被攻擊的次數曲線圖，橫軸：時間(共 24 小時)、縱軸：攻擊次數。
- (2) 詳細結果：詳細列出被攻擊的來源 IP、目標 IP、攻擊名稱、時間、風險等資料。
- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊
- \* 點選攻擊名稱可查詢詳細攻擊說明 (圖四 1-3)
- \* Whois 資訊可得知該 IP 所屬國家及 ISP (圖四 1-2)



(圖四 1-2：whois 查詢結果)

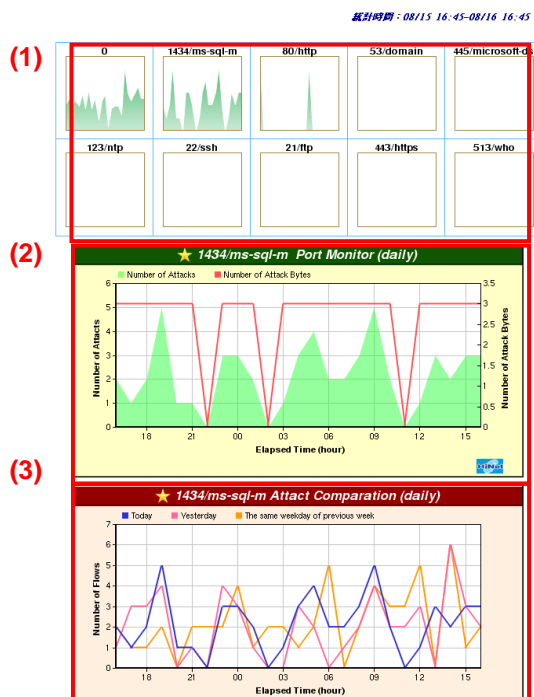


(圖四 1-3：詳細攻擊說明)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 1.2 通訊埠

顯示指定通訊埠 (port) 個別的攻擊次數時間趨勢。



(圖四 1-4：通訊埠)

此頁分三部份：

- (1) **各別通訊埠攻擊趨勢**：每張小圖各代表單一通訊埠在過去 24 小時內被攻擊的次數趨勢圖。用戶可點選其中一張小圖，點選後將會顯示放大圖。
- (2) **攻擊總和趨勢**：攻擊次數大圖，顯示過去 24 小時內被攻擊的次數和攻擊量的統計圖，綠色代表攻擊次數，紅色代表攻擊量。
- (3) **攻擊趨勢比較**：攻擊次數比較圖。藍、紅、橙三條線各代表今日、昨日、及上個禮拜的今日(例如今日為周三，則橙線代表上周三)。用來比較上禮拜、昨日和今日的被攻擊次數的增減趨勢。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

### 1.3 設定

用戶可自行設定需要被監控的通訊埠 (port)，共可指定 10 組通訊埠，用戶可使用下接式選單指定通訊埠，亦可自行輸入通訊埠號。

0	0 / Unknown	00
1	1434 / ms-sql-m	1434
2	80 / http	80
3	53 / domain	53
4	445 / microsoft-ds	445
5	123 / ntp	123
6	22 / ssh	22
7	21 / ftp	21
8	443 / https	443
9	513 / who	513

設定 重置

(圖四 1-5：設定監控通訊埠)

## 2 分析摘要

### 2.1 本日摘要

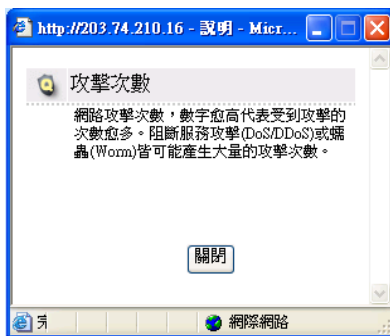
用戶點選後，會列出在過去 24 小時內用戶端被攻擊的詳細資料。



(圖四 2-1：本日摘要)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

- \* 點選右邊的小燈泡可觀看項目說明。
  - \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
  - \* 點選攻擊名稱可查詢詳細攻擊說明
- 項目說明



(圖四 2-2：項目說明)

## 2.2 本日排名

過去 24 小時內的攻擊統計排名。



(圖四 2-3：攻擊統計排名)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

- (1) 攻擊來源 IP 統計圓餅圖：列出前五名的來源 IP，上半部為來源 IP 攻擊的次數統計，下半部為來源 IP 攻擊的流量統計。
  - (2) 攻擊目標 IP 統計圓餅圖：列出前五名的目標 IP，上半部為目標 IP 被攻擊的次數統計，下半部為目標 IP 被攻擊的流量統計。
  - (3) 攻擊名稱的統計圓餅圖：列出前五名的攻擊名稱，上半部為攻擊名稱的次數統計，下半部列出依風險程度來區分的攻擊次數統計。
- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
  - \* 點選攻擊名稱可查詢詳細攻擊說明

### 3 自訂查詢

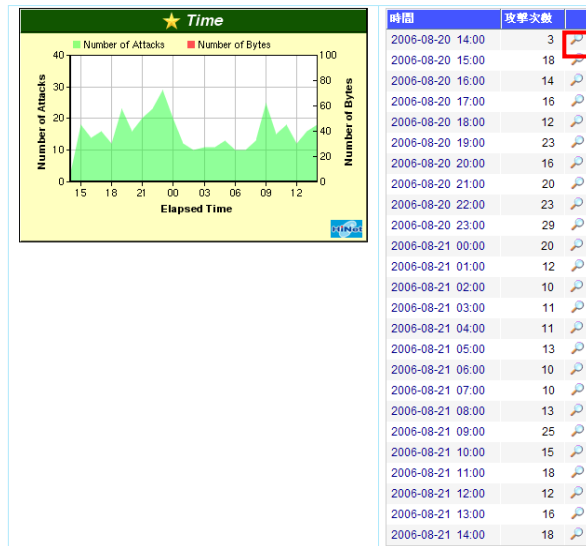
#### 3.1 查詢

用戶可輸入欲查詢的來源 IP、目標 IP、通訊埠、攻擊名稱或時間來查詢詳細的攻擊資料。而輸出的查詢結果可依時間趨勢列出，也可依統計排名列出。

(圖四 3-1：自定查詢)

- a. 依時間趨勢列出：

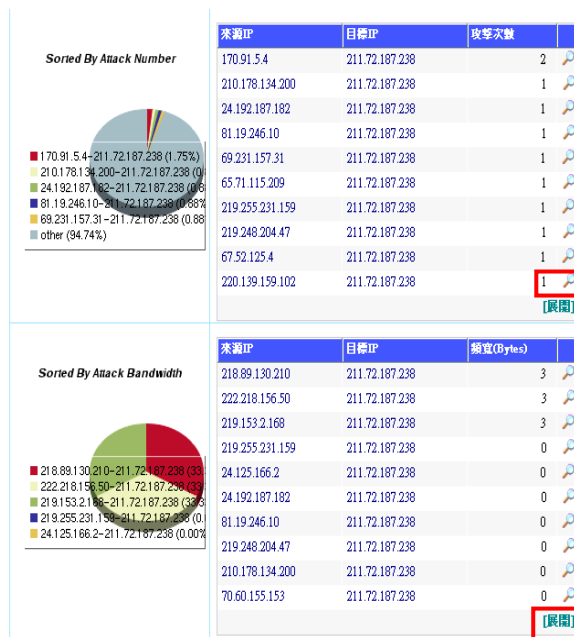
名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0



(圖四 3-2：以時間趨勢呈現查詢結果)

b. 依統計排名列出：

點選列表下方的“**[展開]**”字樣會在新視窗顯示完整列表。點選列表右邊的放大鏡圖示會顯示出詳細的攻擊事件時間。



(圖四 3-3：以統計排名呈現查詢結果)

c. 點擊放大鏡

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

頁 1 of 1

詳細結果				第一頁	上頁	1	下頁	最後一頁
來源IP	目標IP	風險	攻擊名稱	Bytes	時間			
221.185.192.16	211.72.187.236	high	Worm-Welchia_icmp	0	17/08/2006 11:54:45			
218.28.119.69	211.72.187.238	high	Worm-Welchia_icmp	0	17/08/2006 11:55:35			
211.1.193.165	211.72.187.234	high	Worm-Welchia_icmp	0	17/08/2006 11:55:55			

(圖四 3-4：詳細攻擊事件列表)

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

d. 點擊展開

頁 1 of 19

詳細結果		第一頁	上頁	1 下頁	最後一頁
來源IP	目標IP				
219.140.57.37	211.72.187.235	6			
219.140.57.37	211.72.187.232	6			
219.140.57.37	211.72.187.233	6			
219.140.57.37	211.72.187.234	5			
219.140.57.37	211.72.187.236	4			
70.69.139.112	211.72.187.236	1			
203.172.130.98	211.72.187.234	1			
61.15.105.82	211.72.187.238	1			
67.187.17.20	211.72.187.238	1			
202.103.247.148	211.72.187.235	1			
216.105.214.115	211.72.187.239	1			

(圖四 3-5：完整攻擊事件統計排名列表)

- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
- \* 點選攻擊名稱可查詢詳細攻擊說明
- \* 點選列表右邊的放大鏡圖示會顯示出詳細的攻擊事件列表



名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 4 統計報表

### 4.1 日報

觀看每日的攻擊統計報表。



(圖四 4-1：日報表列表)

- \* 點選日曆上的**放大鏡圖示**，可在新視窗看到當日被攻擊的詳細資料。
- \* 統計報表由系統排程定時產生，製作完成後即可於網頁上點選觀看。
- \* 統計報表有保存時限，報表過期後將不在保存於本系統，用戶如有保存需求，請於期限前自行下載或列印。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

a. 日報表內容

**DailyReport(88278311)**

統計時間：2012-05-22 00:00~2012-05-23 00:00

下載PDF
 列印

用戶號碼	88278311	
總阻擋攻擊次數	0 (次)	
總阻擋攻擊流量	0 (Bytes)	
受攻擊通訊埠個數	0	
已阻擋攻擊項目	0	
IP數量	來源IP	0
	目標IP	0
風險	高	
	中	
	低	
攻擊方向	外 → 內	(次)
	內 → 外	(次)

---

**目錄**

1. 每日攻擊阻擋次數
2. 風險等級分布
3. 前10受攻擊通訊埠
4. 前10攻擊項目
5. 前10攻擊來源IP

(圖四 4-2：日報表內容)

- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
- \* 點選攻擊名稱可查詢詳細攻擊說明

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 4.2 週報

觀看每周的攻擊統計報表。



(圖四 4-3：週報表列表)

- \* 點選日曆上的**放大鏡圖示**，可在新視窗看到當周攻擊統計詳細資料。
- \* 統計報表由系統排程定時產生，製作完成後即可於網頁上點選觀看。
- \* 統計報表有保存時限，報表過期後將不在保存於本系統，用戶如有保存需求，請於期限前自行下載或列印。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

a. 周報表內容

**WeeklyReport(88278311)**

統計時間：2012-05-14 00:00~2012-05-21 00:00

 下載PDF
  列印

用戶號碼	88278311						
總阻擋攻擊次數	0 (次) 						
總阻擋攻擊流量	0 (Bytes) 						
受攻擊通訊埠個數	0 						
已阻擋攻擊項目	0						
IP數量	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>來源IP</td> <td>0</td> </tr> <tr> <td>目標IP</td> <td>0</td> </tr> </table>	來源IP	0	目標IP	0		
來源IP	0						
目標IP	0						
風險	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>高</td> <td></td> </tr> <tr> <td>中</td> <td></td> </tr> <tr> <td>低</td> <td></td> </tr> </table>	高		中		低	
高							
中							
低							
攻擊方向	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>外 → 內</td> <td>(次) </td> </tr> <tr> <td>內 → 外</td> <td>(次)</td> </tr> </table>	外 → 內	(次) 	內 → 外	(次)		
外 → 內	(次) 						
內 → 外	(次)						

**目錄**

1. [每日攻擊阻擋次數](#)
2. [風險等級分布](#)
3. [前20受攻擊通訊埠](#)
4. [前20攻擊項目](#)
5. [前20攻擊來源IP](#)

(圖四 4-4：週報表內容)

- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
- \* 點選攻擊名稱可查詢詳細攻擊說明

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

### 4.3 月報

觀看每月的攻擊統計報表。



(圖四 4-5：月報表列表)

- \* 點選日曆上的**放大鏡圖示**，可在新視窗看到當周攻擊統計詳細資料。
- \* 統計報表由系統排程定時產生，製作完成後即可於網頁上點選觀看。
- \* 統計報表有保存時限，報表過期後將不在保存於本系統，用戶如有保存需求，請於期限前自行下載或列印。

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

b. 月報表內容



(圖四 4-6：月報表內容)

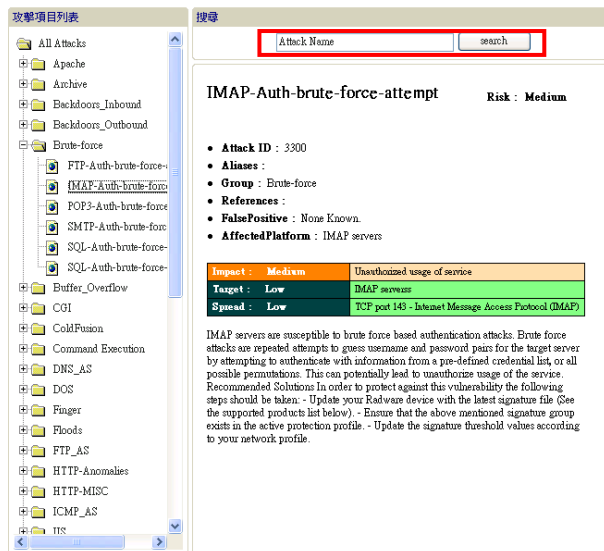
- \* 點選來源 IP、目標 IP 可查詢 Whois 資訊。
- \* 點選攻擊名稱可查詢詳細攻擊說明

名稱	HiNet網路入侵防護服務報表說明書	安全等級	公開
編號		版次	V1.0

## 5 說明

### 5.1 攻擊資料庫

用戶可點選左邊樹狀選單，已觀看攻擊項目的完整介紹。亦可利用自行輸入關鍵字來查詢。



### 5.2 問答集

此頁提供了一些用戶常見疑問及問答。

即時監控(Monitor) 分析摘要(Analysis) 自訂查詢(Query) 統計報表(Report) 說明(Help)

攻擊資料庫 問答集

- 什麼是入侵防護服務?
- 我已經自行建置IPS設備了，為什麼還需要網路入侵防護服務?
- 入侵防護服務有何特色?
- 為什麼我會有內對外的攻擊事件?
- 要怎麼判斷觸發的事件是真的有問題，還是誤判?
- 我的防火牆出現了由同一個來源IP的大量連線紀錄，為什麼IPS報表中沒有出現攻擊log?
- 為什麼沒有收到IPS報表的MAIL?

---

**什麼是入侵防護服務?**

入侵防護服務，係於網路端建置高效能之「入侵防護系統(IPS)」，並由專業資安團隊負責維護，即時阻擋蠕蟲、駭客攻擊等網路型資安威脅，以提供企業或政府機關第一道的安全防護。

[ Top ]

---

**我已經自行建置IPS設備了，為什麼還需要網路入侵防護服務?**

本服務於ISP網路端阻擋惡意攻擊，可減少攻擊行為佔用你寶貴的頻寬，並可與你自行建置之IPS設備相輔相成，防護功能及項目互補，提高防護率。

[ Top ]

~ 感謝您租用 HiNet 入侵防護服務! ~