

NetSecure

區域網路安全控管解決方案

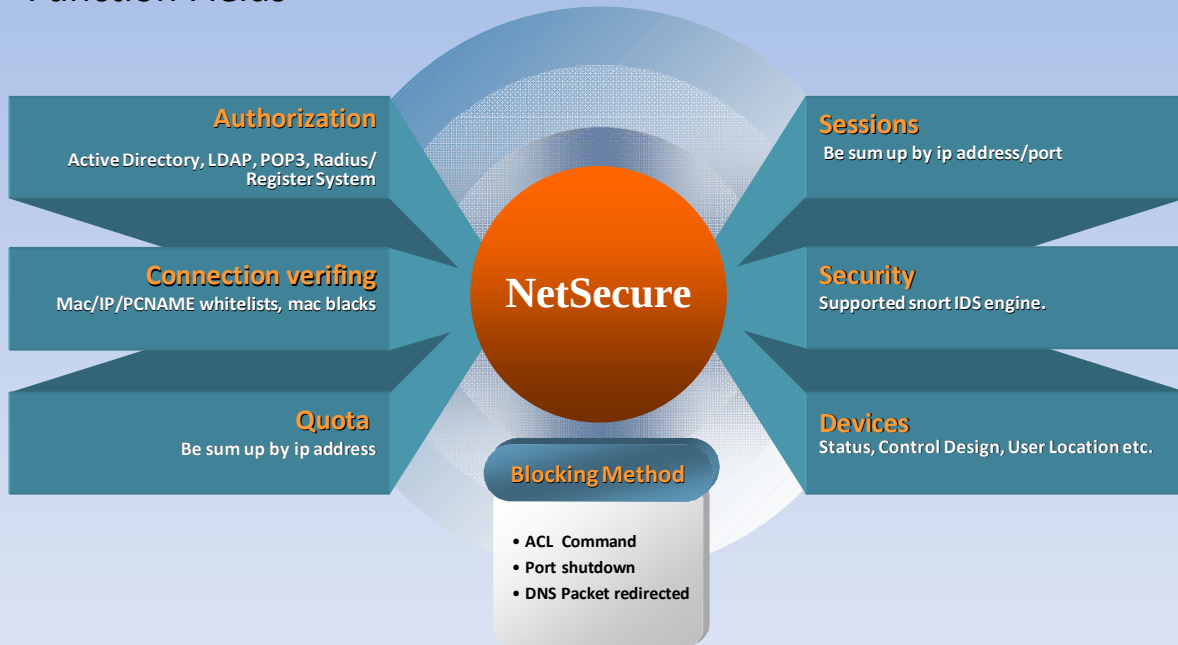
一休資訊科技股份有限公司

1. 如何透過集中式的方式管理IP/Mac/PC name
2. 區域網路上身份識別與存取管理
3. 區域網路異常流量分析及管控
4. 如何透過長期網路流量報表提供稽查與紀錄

一休資訊科技股份有限公司

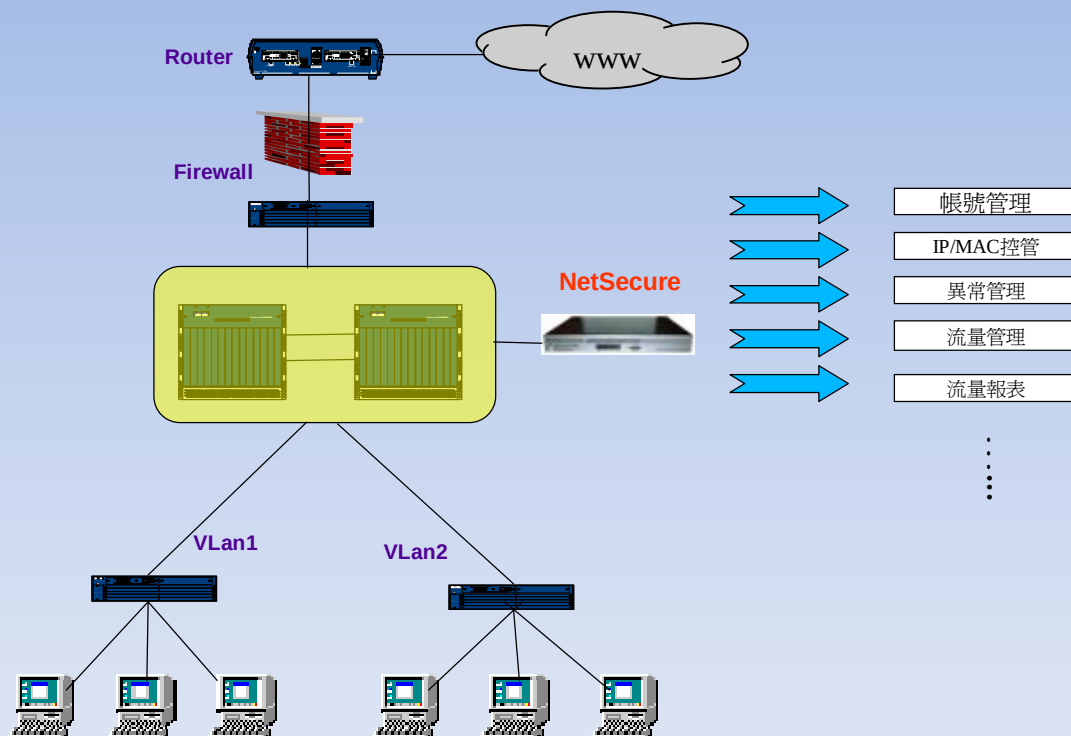
NetSecure

Function Fields



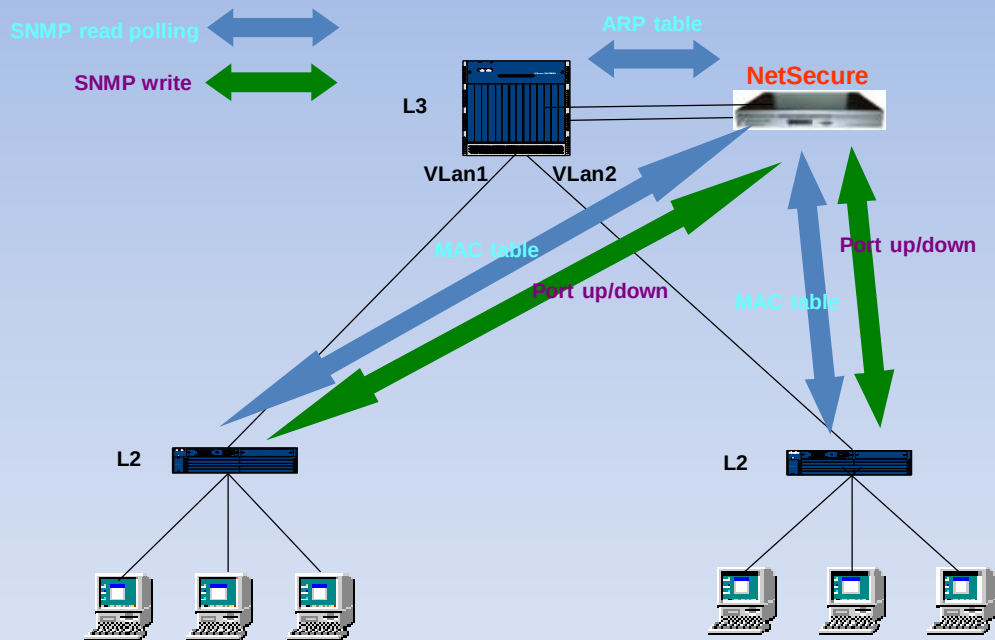
一休資訊科技股份有限公司

NetSecure 架構圖



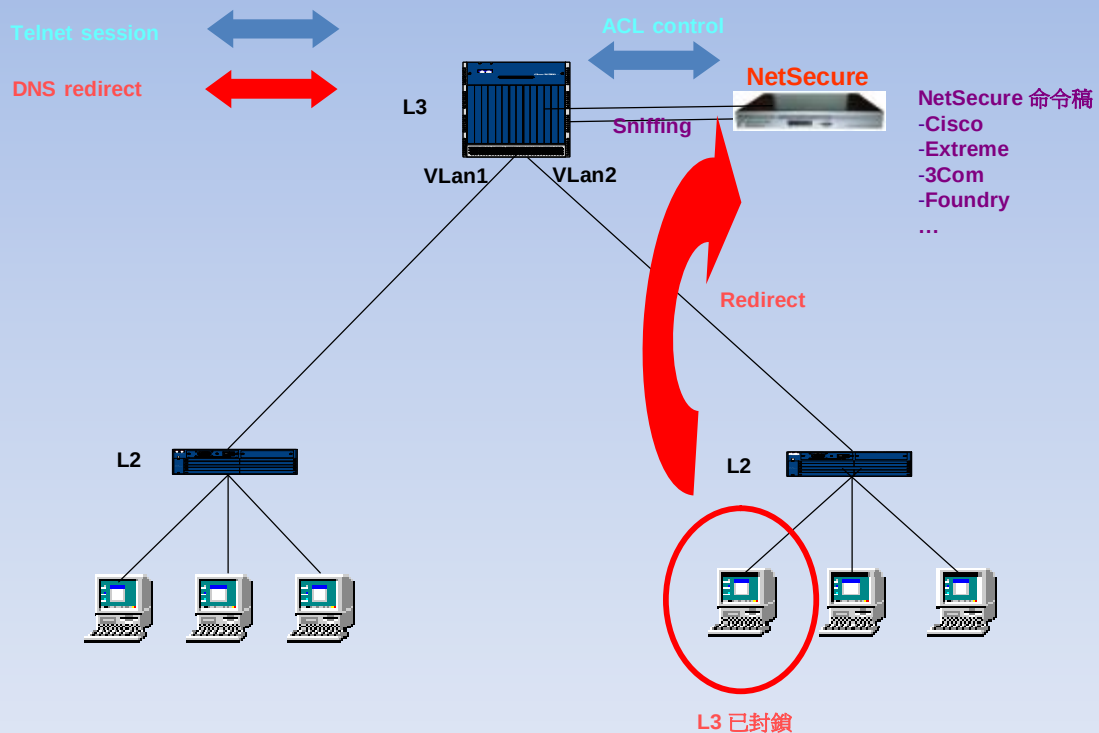
一休資訊科技股份有限公司

NetSecure 與 SNMP



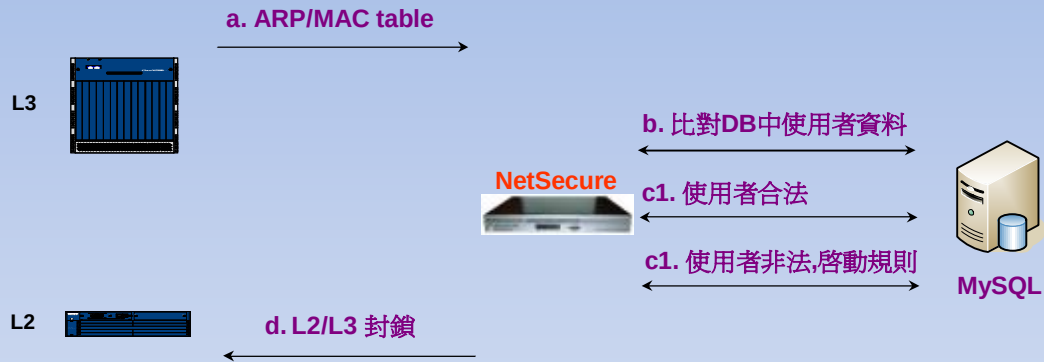
一休資訊科技股份有限公司

NetSecure 與 Telnet



一休資訊科技股份有限公司

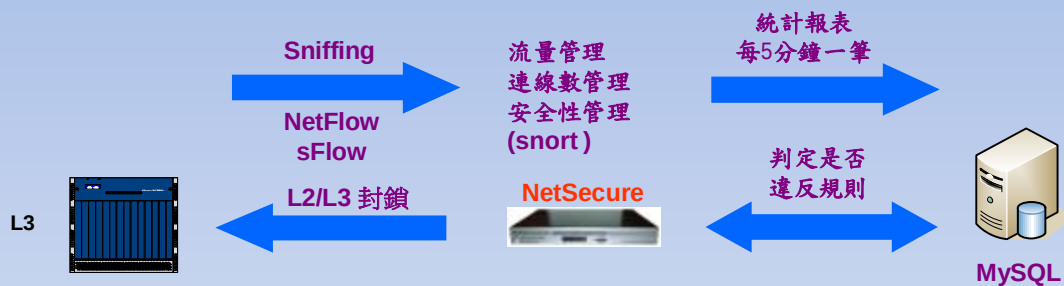
NetSecure 帳號及IP-MAC管理



- c1. 依規則可設定L2或L3封鎖
- L2封鎖會自動比對DB中, 違規IP -> ARP -> MAC 的資料
 - L3封鎖會依照自訂的命令稿以及L3設定發送ACL命令

一休資訊科技股份有限公司

NetSecure 流量管理

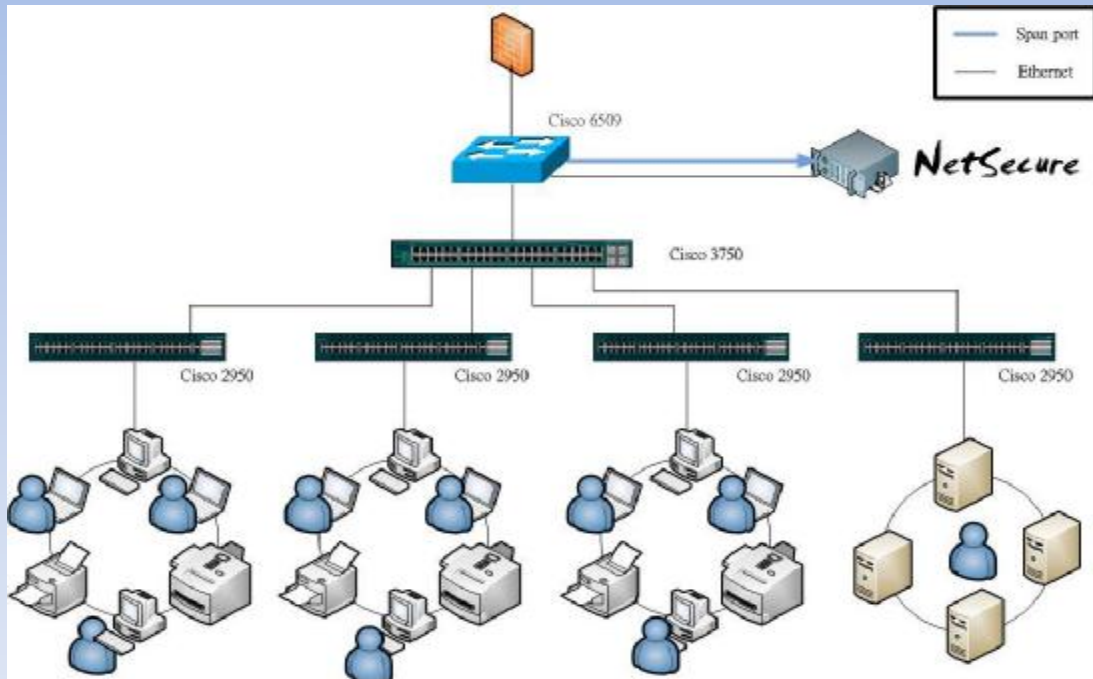


- 依規則可設定
- a. L2/L3 封鎖
 - b. 封鎖次數
 - c. 封鎖時間長短
- 並可套用於不同單位群組使用不同的規則管理

一休資訊科技股份有限公司

NetSecure

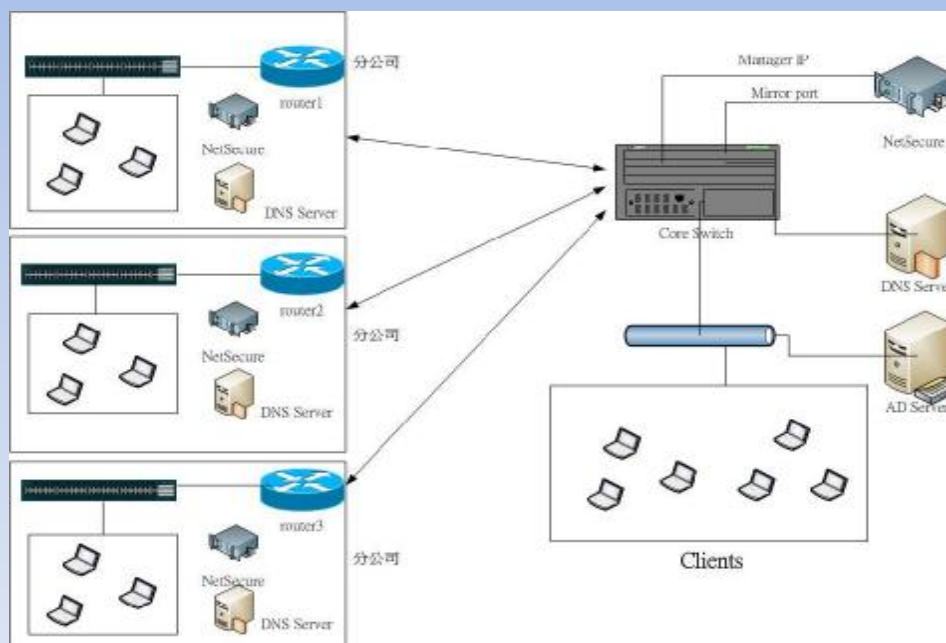
Basic network frame diagram



一休資訊科技股份有限公司

NetSecure

Distributed frame diagram



一休資訊科技股份有限公司

NetSecure

功能簡介

- ◎身份識別與網路存取
- ◎IP-MAC白名單
- ◎使用量管理
- ◎連線數管理
- ◎異常連線管理
- ◎網路設備
- ◎使用者狀態
- ◎封鎖與導向
- ◎報表與紀錄

一休資訊科技股份有限公司

NetSecure

功能簡介-身份識別與網路存取

- ◎提供註冊系統。使用者上線均需先註冊通過後才能獲得網路使用權。
- ◎支援AD、LDAP、POP3、RADIUS等主要認證伺服器。使用者上線均須通過認證後才能獲得網路使用權。

The screenshot displays the NetSecure web interface for user management. At the top, a breadcrumb trail reads: 首頁 >> 系統管理 >> 註冊/認證伺服器管理. Below this, there are several sections for configuration:

- 請選擇一種管理方式:** Includes radio buttons for 註冊 (selected) and 認證.
- 請選擇一種驗證模組:** Includes radio buttons for 對組 and 單位.
- 請選擇一種認證方式:** Includes radio buttons for AD Domain, LDAP, AD, POP3 (selected), and Radius.
- 登入認證方式:** Includes radio buttons for 驗證 and 離網.

Below these options, there is a text input field for the username and a dropdown menu for the unit, followed by a 次 (times) button. A note at the bottom states: 登入系統人員以AD或LDAP伺服器為主, 同一單位最多可註冊/認證 1 次.

一休資訊科技股份有限公司

NetSecure

功能簡介-IP/MAC白名單

◎提供數種組合白名單，不符合者無法獲得網路存取權

首頁 >> 封鎖/警告設定 >> 連線驗證管理						
資料共 (41) 筆 顯示數目 (3) 頁						
全選	單位	使用者ID	PC NAME	IP	MAC	備註
☐	FIEND TEST		CENTER	10.1.1.1	000fa3e4b80	
☐	FIEND TEST		EQ-WEB	10.1.1.2	00e04cd809ad	
☐	FIEND TEST			10.1.1.5	0018fe9bffa7	
☐	FIEND TEST			10.1.1.6	0010f386e31f	
☐	FIEND TEST		LIH	10.1.1.18	0050baccf12e	
☐	FIEND TEST		SUPPORTSERVERII	10.1.1.19	0016e6d4eda2	
☐	FIEND TEST		EQ-AME	10.1.1.20	0020e0604c9e	
☐	FIEND TEST		KENQQ	10.1.1.21	00137216a687	
☐	FIEND TEST			10.1.1.31	000c2970667c	
☐	FIEND TEST			10.1.1.65	000c29b173fe	
☐	FIEND TEST			10.1.1.66	000c29abc0ca	
☐	FIEND TEST		EQT-ACS	10.1.1.67	000c29c4bac7	
☐	FIEND TEST			10.1.1.71	000e2eef0232	
☐	FIEND TEST			10.1.1.111	000dc8082a98	
☐	FIEND TEST			10.1.1.112	000dc8081cab	
☐	FIEND TEST			10.1.1.155	001d7da6395e	
☐	FIEND TEST			10.1.1.160	000c29e16c06	
☐	FIEND TEST			10.1.1.167	000c29097ecb	
☐	FIEND TEST			10.1.1.171	000c29fde5a	
☐	FIEND TEST			10.1.1.175	000c29103649	

一休資訊科技股份有限公司

NetSecure

功能簡介-使用量管理

首頁 >> 封鎖/警告設定 >> 流量限制時段設定						
資料共 (15) 筆 顯示數目 (1) 頁						
限制時段名稱	封鎖方式	告警解除級別	封鎖設備	封鎖對象	時間設定	修改 刪除
流量限制 L2	自動	每次封鎖三分鐘,第三次 永遠封鎖	封鎖L2	針對電腦 MAC	設定	
流量限制test2	自動	第一次1小時,第二次1 天,第三次一個月	封鎖L3	針對電腦 MAC	設定	
流量限制test3	自動	第一次1小時,第二次1 天,第三次一個月	封鎖L3	針對電腦 MAC	設定	

首頁 >> 流量限制時段 >> 流量限制時段							
資料共 (1) 筆 顯示數目 (1) 頁							
全選	單位	封鎖對象	設備ID (IMEI)	告警方式	封鎖設備	封鎖時間範圍	流量限制數量
☐	測試2	針對MAC (001303c0f1d)	測試 設備ID: 001303c0f1d	封鎖區	封鎖L3	2007-05-10 0:15 - 5	2007-05-10 00:15:00
☐	測試3	針對MAC (001303c0f1d)	測試 設備ID: 001303c0f1d	封鎖區	封鎖L3	2007-05-10 0:15:00 - 5	2007-05-10 00:15:00

一休資訊科技股份有限公司

NetSecure

功能簡介-連線數管理

首頁 >> 封鎖/警告設定 >> 連線異常規則設定							資料共 [15] 筆 總頁數共 [1] 頁	
規則名稱	封鎖方式	客製化封鎖規則	封鎖路徑	封鎖對象	偵測通訊埠	連線數	修改	刪除
連線異常test	自動	每次封鎖三分鐘,第三次永遠封鎖	封鎖L3	針對 IP	所有通訊埠			
連線異常 test2	自動	第一次1小時,第二次1天,第三次一個月	封鎖L3	針對身份	所有通訊埠			
連線異常test3	自動	每次封鎖三分鐘,第三次永遠封鎖	封鎖L3	針對MAC	指定通訊埠	設定		

一休資訊科技股份有限公司

NetSecure

功能簡介-異常連線管理

首頁 >> 封鎖/警告設定 >> 安全性封鎖規則							資料共 [3] 筆 總頁數共 [1] 頁	
規則名稱	封鎖方式	客製化封鎖規則	封鎖路徑	安全性	修改	刪除		
安全性(高)	自動	5,10,15	封鎖L2	高安全性				
安全性(中)	自動	5,10,15	封鎖L3	中安全性				
安全性(超序)	自動	前1次鎖3分鐘第二次後每次鎖5之指數	封鎖L3	超序安全性				

一休資訊科技股份有限公司

流量管理

1. 每個IP位址可依用途給予不同之流量quota 限制
2. 流量限制可依不同網段管制並統計其流量
3. 超過流量限制時，即對該IP管制網路存取，並MAIL通知管理者，或限制可連線範圍、阻斷IP等。並將違規事件，記錄於資料庫中
4. 提供每個IP位址每日流量總數及TOP N 報表
5. 對於流量異常之IP可設定阻斷時間與次數，自動或人工阻斷

時間	來源單位	來源	目的地	連線數	封包數	流量 / K
2007-03-30 00:50:00	單位1 10.1.1.4	10.1.1.134	單位1 10.1.1.20	9	197	04.56
2007-03-30 00:50:00	單位1 10.1.1.4	10.1.1.10	單位1 10.1.1.191	81	2841	282.95
2007-03-30 00:45:00	單位1 10.1.1.4	10.1.1.19	單位1 10.1.1.255	1	1	0.08
2007-03-30 00:45:00	單位1 10.1.1.4	10.1.1.20	單位1 10.1.1.19	3	3	0.12
2007-03-30 00:45:00	單位1 10.1.1.4	10.1.1.18	單位1 10.1.1.20	3	3	0.15
2007-03-30 00:45:00	單位1 10.1.1.4	10.1.1.20	單位1 10.1.1.1	1	1	0.23
2007-03-30 00:45:00	單位1 10.1.1.4	10.1.1.20	單位1 10.1.1.255	1	1	0.22

一休資訊科技股份有限公司

流量時段限制規則(可設定時段及使用量)

限制時段名稱	開始時間	結束時間	流量限制 (M)	修改	刪除
流量限制test	01:00:00	06:00:00	1		
流量限制test	06:00:01	12:00:00	50		
流量限制test	12:00:01	19:00:00	100		

流量限制50M

封鎖對象為MAC

限制時段名稱	封鎖方式	含解除封鎖規則	封鎖設備	封鎖對象	時間設定	修改	刪除
流量限制test	自動	每次三分鐘,第四次永遠封鎖	封鎖L3	針對電腦-MAC			
流量限制test2	自動	每次三分鐘,第四次永遠封鎖	封鎖L3	針對 IP			

一休資訊科技股份有限公司

網路異常管理功能

1. 偵測已知之網路攻擊型病毒（如Blaster、Welicha、Goabot等）、P2P連線、駭客攻擊、Session過多、packet過多等類別之連線，且依危險等級提供不同之處置方式
2. 系統應區分為安全區、警示區（發出警告，繼續監視，不阻斷其使用網路）、阻斷區（阻斷使用者使用網路）



一休資訊科技股份有限公司

異常偵測設定規則功能

使用者可手動新增或開啟/關閉,所要偵測的異常封包項目

全選	代碼	名稱	開啟或關閉	規則內容
☒	attack-responses	attack-responses	☒	詳細內容
☒	backdoor	backdoor	☒	詳細內容
☒	bad-traffic	bad-traffic	☒	詳細內容
☒	chat	chat	☒	詳細內容
☒	ddos	ddos	☒	詳細內容
☒	deleted	deleted	☒	詳細內容
☒	dns	dns	☒	詳細內容
☒	dos	dos	☒	詳細內容
☒	experimental	experimental	☒	詳細內容
☒	exploit	exploit	☒	詳細內容
☒	finger	finger	☒	詳細內容
☒	ftp	ftp	☒	詳細內容
☒	icmp	icmp	☒	詳細內容
☒	icmp-info	icmp-info	☒	詳細內容
☒	imap	imap	☒	詳細內容

一休資訊科技股份有限公司

封包異常行為記錄(使用MSN行為)

首頁 >> 系統警示記錄查詢 >> 封包異常記錄

資料共 [12] 筆，總頁數共 [3] 頁

全選	全不選	來源IP	來源PORT	目標IP	目標PORT	通訊協定	次數	攻擊方式	開始時間	結束時間
☐	☐	10.1.2.100	3074	207.46.27.29	1063	TCP : 6	1	CHAT MSN user search	2006-09-15 15:50:09	2006-09-15 15:50:09
☐	☐	10.1.2.77	2204	10.1.1.177	80	TCP : 6	6	(http inspect) OVERSIZE....	2006-09-15 15:52:30	2006-09-15 15:54:16
☐	☐	10.1.2.203	1024	239.255.255.255	1900	UDP : 17	11	MISC UPnP malformed....	2006-09-15 15:55:13	2006-09-15 15:55:13
☐	☐	10.1.2.248	0	222.88.250.189	0	ICMP : 1	3	ICMP Destination....	2006-09-15 16:00:32	2006-09-15 16:00:32
☐	☐	61.135.146.207	32767	10.1.2.203	80	TCP : 8	2	WEB-MISC robots.txt access	2006-09-15 16:01:50	2006-09-15 16:01:50
☐	☐	10.1.2.248	0	222.43.113.58	0	ICMP : 1	12	ICMP Destination....	2006-09-15 16:10:23	2006-09-15 16:10:23
☐	☐	10.1.2.114	1870	10.1.1.1	139	TCP : 6	17	NETBIOS SMB IPC\$... unhandled....	2006-09-15 16:00:14	2006-09-15 16:12:14

違反MSN傳輸行為

違反ICMP傳輸行為
(執行檔案交換軟體)

一休資訊科技股份有限公司

疑似中毒清單(攻擊方式)

首頁 >> 系統警示記錄查詢 >> 安全性異常記錄 >> 安全性封包異常清單

資料共 [6] 筆，總頁數共 [1] 頁

全選	全不選	來源IP	來源PORT	目標IP	目標PORT	通訊協定	次數	攻擊方式	開始時間	結束時間
☐	☐	10	1602	10	445	TCP : 6	3	NETBIOS SMB-DS IPC\$....	2006-07-05 16:14:48	2006-07-05 16:14:48
☐	☐	10	1602	10	445	TCP : 6	3	NETBIOS SMB-DS Session....	2006-07-05 16:14:48	2006-07-05 16:14:48
☐	☐	10	0	10	0	ICMP : 1	6	ICMP PING	2006-07-05 16:14:48	2006-07-05 16:14:48
☐	☐	10	0	10	0	ICMP : 1	4	ICMP L3retriever Ping	2006-07-05 16:14:48	2006-07-05 16:14:48
☐	☐	10	0	10	0	ICMP : 1	3057	ICMP PING	2006-07-05 16:09:01	2006-07-05 16:26:01
☐	☐	10	0	10	0	ICMP : 1	3057	ICMP PING Windows	2006-07-05 16:09:01	2006-07-05 16:26:01

一休資訊科技股份有限公司

NetSecure

功能簡介-網路設備



The screenshot shows the 'Network Device Management' section of the NetSecure interface. At the top, there is a breadcrumb trail: 'Home >> Network Device Management >> Device Interface Control'. A search bar on the right shows '設備: I-CISCO3550' with a '搜尋' (Search) button. Below the breadcrumb, it indicates '資料共 (54) 筆' (Total 54 records) and '顯示數共 (3) 頁' (Total 3 pages). The main table lists network devices with columns for '設備' (Device), '編號' (ID), '說明' (Description), '管理狀態' (Management Status), and '連接狀態' (Connection Status). All devices are of type 'CISCO3550' and have a 'FastEthernet0/1' through 'FastEthernet0/10' interface. The management status is represented by a green circle with a checkmark, and the connection status is represented by a green circle with a plus sign.

設備	編號	說明	管理狀態	連接狀態
CISCO3550	1	FastEthernet0/1		
CISCO3550	2	FastEthernet0/2		
CISCO3550	3	FastEthernet0/3		
CISCO3550	4	FastEthernet0/4		
CISCO3550	5	FastEthernet0/5		
CISCO3550	6	FastEthernet0/6		
CISCO3550	7	FastEthernet0/7		
CISCO3550	8	FastEthernet0/8		
CISCO3550	9	FastEthernet0/9		
CISCO3550	10	FastEthernet0/10		

一休資訊科技股份有限公司

NetSecure

功能簡介-使用者狀態-ARP TABLE



The screenshot shows the 'IP&MAC(ARP)' section of the NetSecure interface. The breadcrumb trail is 'Home >> System Management >> IP&MAC(ARP)'. It indicates '資料共 (48) 筆' (Total 48 records) and '顯示數共 (2) 頁' (Total 2 pages). The table has columns for '設備名稱' (Device Name), '單位' (Unit), 'IP', 'MAC', 'PC NAME', '修改時間' (Modification Time), and '備註' (Remarks). The '設備名稱' column has a dropdown menu set to '全區' (All). The '單位' column has a dropdown menu set to 'FIEND TEST'. The 'IP' column shows various IP addresses, and the 'MAC' column shows corresponding MAC addresses. The 'PC NAME' column shows names like 'CENTER', 'EQ-WEB', 'LJH', 'SUPPORTSERVERII', 'EQ-AME', 'KENQQ', and 'EQIT-ACS'. The '修改時間' column shows dates from 2008-02-18 to 03-23-13. The '備註' column has a dropdown menu set to '全區'.

設備名稱	單位	IP	MAC	PC NAME	修改時間	備註
CISCO3550	FIEND TEST	10.1.1.1	000fa23e4b80	CENTER	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.2	00e04cd00ad	EQ-WEB	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.5	0018fe9bffa7		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.6	0010f306e31f		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.18	0050baccf12e	LJH	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.19	0016e6d4eda2	SUPPORTSERVERII	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.20	0020e6604c96	EQ-AME	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.21	00137216a697	KENQQ	2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.31	000c2976667e		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.60	0016e6d48b3e		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.65	000c29b173fe		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.66	000c29abc8ca		2008-02-18 03:23:13	
CISCO3550	FIEND TEST	10.1.1.67	000c29c4bac7	EQIT-ACS	2008-02-18 03:23:13	

一休資訊科技股份有限公司

NetSecure

功能簡介-使用者狀態-AD認證紀錄



一休資訊科技股份有限公司

NetSecure

功能簡介-使用者狀態-使用者位置查詢



一休資訊科技股份有限公司

NetSecure

功能簡介-例外名單



一休資訊科技股份有限公司

NetSecure

功能簡介-資料庫管理



一休資訊科技股份有限公司

NetSecure

功能簡介-重導畫面設置



一休資訊科技股份有限公司

NetSecure

功能簡介-封鎖與導向

◎ACL Command:

- 尋找所在的Level 3 Switch，封鎖目標。
- 支援的Switch 廠牌如下(支援ACL指令者)
 - Cisco
 - Foundry
 - Extreme
 - Nortel(限8600)
 - 3COM(8810)
 - HP(特定型號)

一休資訊科技股份有限公司

NetSecure

功能簡介-封鎖與導向

◎Port Shutdown:

- 尋找到最下層的Level 2 Switch，對目標所在的port做shutdown封鎖。
- 限支援SNMP協定之網路設備(Switch)

◎DNS Packet Redirect:

為預設之封鎖干擾方式，原用途為將違規IP導向至NetSecure訊息頁，但在不影響實際SW時可用來做干擾封鎖使用。(須視環境做配置)

一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

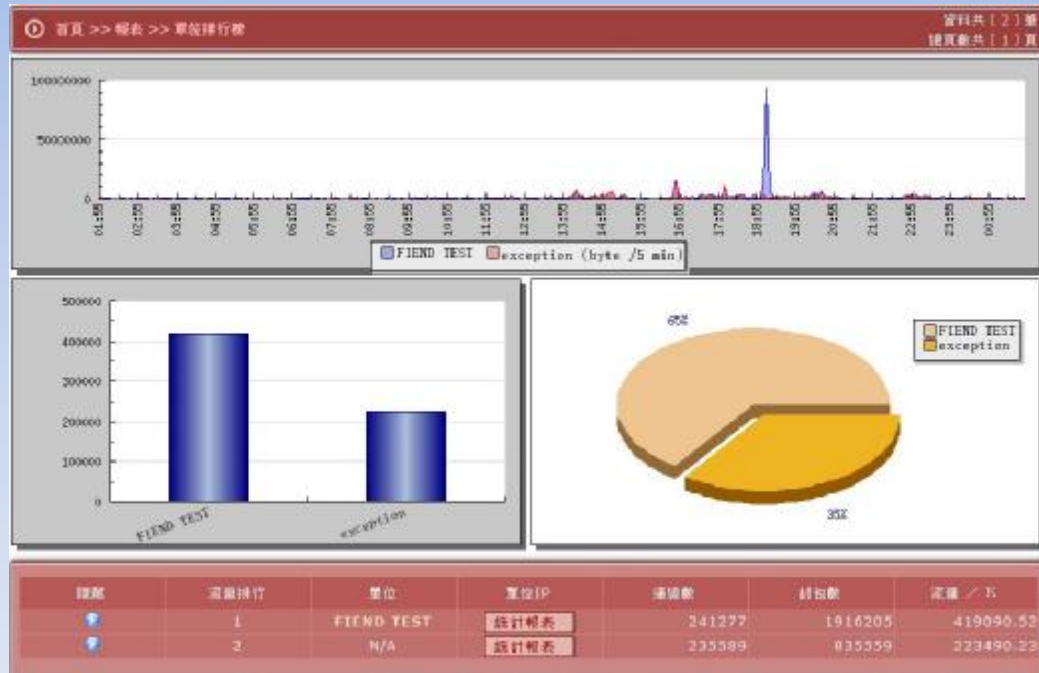
功能簡介-報表



一休資訊科技股份有限公司

NetSecure

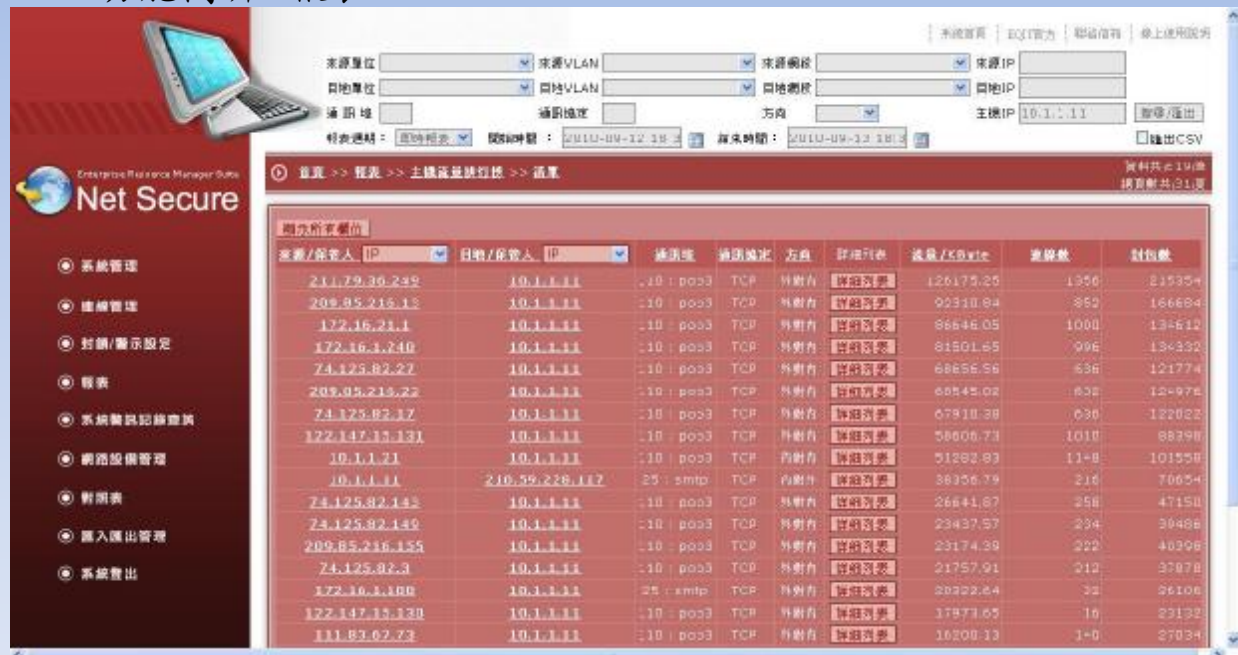
功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表



一休資訊科技股份有限公司

NetSecure

功能簡介-報表

來源單位: [] 來源VLAN: [] 來源網段: [] 來源IP: []
 目標單位: [] 目標VLAN: [] 目標網段: [] 目標IP: []
 通訊埠: [] 通訊埠範圍: [] 方向: [] 主機IP: []
 報表週期: [] 開始時間: 2010-09-12 16:12 結束時間: 2010-09-12 16:12
 ☐ 匯出CSV

首頁 >> 報表 >> 系統通訊埠 >> 匯出列表

來源單位	來源VLAN	來源網段	來源IP	目標單位	目標VLAN	目標網段	目標IP	通訊埠	通訊埠範圍	方向	通訊數	封包數	流量/K	日期/時間
N/A	N/A	N/A	10.1.15.3	N/A	N/A	N/A	74.54.4.55	80: http	TCP	其它	90532.43	15512189	13	2310-09-13 15:35:30
N/A	N/A	N/A	10.1.10.101	N/A	N/A	N/A	202.39.235.131	80: http	TCP	其它	26910.42	224	35497	13
N/A	N/A	N/A	10.1.10.101	N/A	N/A	N/A	202.39.235.131	80: http	TCP	其它	16198.30	132	27954	13
N/A	N/A	N/A	10.1.15.3	N/A	N/A	N/A	69.4.231.52	80: http	TCP	其它	15815.24	78	31597	13
N/A	N/A	N/A	10.1.10.101	N/A	N/A	N/A	123.193.232.195	80: http	UDP	其它	13094.57	120	16776	13
N/A	N/A	N/A	38.107.114.102	N/A	N/A	N/A	10.1.10.101	443: https	UDP	其它	12134.54	120	35273	13
N/A	N/A	N/A	38.107.114.102	N/A	N/A	N/A	10.1.10.101	443: https	UDP	其它	11914.46	120	26076	13
N/A	N/A	N/A	38.107.114.102	N/A	N/A	N/A	10.1.10.101	443: https	UDP	其它	11804.17	120	27381	13

一休資訊科技股份有限公司

NetSecure

功能簡介-警示紀錄



一休資訊科技股份有限公司

NetSecure

功能簡介-IP狀態

首頁 >> 系統警訊記錄查詢 >> IP狀態查詢										
資料共 142 筆 總頁數共 3 頁										
全選	封鎖	單位	顯示	使用狀態	管制狀態	警示	封鎖	封鎖時間	自動解封	最新封鎖原因
全不選	全解封		IP							
☐		FIEND TEST	10.1.1.1	IP 使用中 MAC:000fe3e40d00	安全區	0	0		0	
☐		FIEND TEST	10.1.1.2	IP 使用中 MAC:00e04cdd09ad	安全區	0	0		0	
☐		FIEND TEST	10.1.1.5	IP 使用中 MAC:0018fa9b007	安全區	0	0		0	
☐		FIEND TEST	10.1.1.6	IP 使用中 MAC:0010f306e31f	安全區	0	0		0	
☐		FIEND TEST	10.1.1.18	IP 使用中 MAC:0050baccf12e	安全區	0	0		0	
☐		FIEND TEST	10.1.1.19	IP 使用中 MAC:0010e6d4eda2	安全區	0	0		0	
☐		FIEND TEST	10.1.1.20	IP 使用中 MAC:0020e0604c96	安全區	0	0		0	
☐		FIEND TEST	10.1.1.21	IP 使用中 MAC:00137216a697	安全區	0	0		0	
☐		FIEND TEST	10.1.1.31	IP 使用中 MAC:000c2976667c	安全區	0	0		0	
☐		FIEND TEST	10.1.1.60	IP 使用中 MAC:0016e6d40b3e	安全區	0	0		0	
☐		FIEND TEST	10.1.1.63	IP 使用中 MAC:000c29b173fe	安全區	0	0		0	

一休資訊科技股份有限公司

NetSecure

功能簡介-黑名單



一休資訊科技股份有限公司

NetSecure

功能簡介-操作紀錄



一休資訊科技股份有限公司

NetSecure

- 非法使用者I：
此功能提供所有曾經被封鎖或解除封鎖歷史記錄查詢，當『違規設定』中 AD 認證功能開啟，未經AD認證而嘗試使用網路者，將會被系統列入非法使用者，進而封鎖。



一休資訊科技股份有限公司

NetSecure

- 非法使用者II：
被封鎖後，瀏覽器自動導向的畫面。



一休資訊科技股份有限公司

NetSecure

- 非法IP-MAC：
此功能根據違規設定中的連線驗證管理，將未符合白名單而遭到封鎖的使用者，加以記錄，管理者可以查詢非法IPMAC的違規或封鎖記錄。

[illegible]

一休資訊科技股份有限公司

NetSecure

- 流量異常記錄：
當使用流量超過管理者定義的大小時，系統將對此IP發出警訊以及啟動封鎖，並通知系統管理員，使用者開啟瀏覽器時將會被自動導向並告知被封鎖原因。

[illegible]

一休資訊科技股份有限公司

NetSecure

- 連線異常記載：
使用者連線數超過管理者定義之大小時，系統將對此 IP 發出警訊以及啟動封鎖，並通知系統管理員，使用者開啟瀏覽器時將會被自動導向並告知被封鎖之原因。



The screenshot shows the NetSecure management console. At the top, there are search filters for 'IP', 'Time', and 'Status'. Below the filters, a table lists connection anomalies. The table has columns for 'Serial', 'IP', 'Anomaly Type', 'Anomaly Description', 'Anomaly Time', 'Anomaly Status', 'Anomaly Count', and 'Anomaly Detail'. The table contains several rows of data, including entries for 'IP: 10.1.2.1' and 'IP: 10.1.2.2'.

序號	IP	異常類型	異常描述	異常時間	異常狀態	異常次數	異常詳情
1	10.1.2.1	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
2	10.1.2.2	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
3	10.1.2.1	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
4	10.1.2.2	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
5	10.1.2.1	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
6	10.1.2.2	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
7	10.1.2.1	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
8	10.1.2.2	連線異常	連線數超過管理者定義之大小	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00

一休資訊科技股份有限公司

NetSecure

- 安全性異常記錄：
記錄使用者的異常的網路行為，如果異常的次數超過管理者定義的大小，系統將對此 IP 發出警訊以及啟動封鎖，並通知系統管理員，使用者開啟瀏覽器時將會被自動導向並告知被封鎖之原因。



The screenshot shows the NetSecure management console. At the top, there are search filters for 'IP', 'Time', and 'Status'. Below the filters, a table lists security anomalies. The table has columns for 'Serial', 'IP', 'Anomaly Type', 'Anomaly Description', 'Anomaly Time', 'Anomaly Status', 'Anomaly Count', and 'Anomaly Detail'. The table contains several rows of data, including entries for 'IP: 10.1.2.1' and 'IP: 10.1.2.2'.

序號	IP	異常類型	異常描述	異常時間	異常狀態	異常次數	異常詳情
1	10.1.2.1	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
2	10.1.2.2	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
3	10.1.2.1	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
4	10.1.2.2	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
5	10.1.2.1	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
6	10.1.2.2	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
7	10.1.2.1	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00
8	10.1.2.2	安全異常	安全異常	2008-08-08 10:00:00	封鎖	1	2008-08-08 10:00:00

一休資訊科技股份有限公司

NetSecure

- 封包異常記錄：
提供違規攻擊者的來源
IP、來源PORT、目的地IP、
目的地PORT、異常原因等資
訊，協助系統管理者了解
其異常網路的行為。



一休資訊科技股份有限公司

NetSecure

功能簡介-警示紀錄



一休資訊科技股份有限公司

NetSecure

- **系統操作記錄：**
此功能將記錄所有操作人員，管理者登入系統進行新增、修改、刪除等操作變更時，自動紀錄變更資料，以便日後系統稽核備查使用。

打印设置 | 返回系统首页 | 数据清除 | 退出系统维护

地址:		操作人姓名:		操作人ID:	
功能名称:		操作方式:	☒ 删除	操作时间:	

首页 >> 系统维护记录管理 >> 系统操作记录

当前共 10121 条，第 1 页 / 411 页

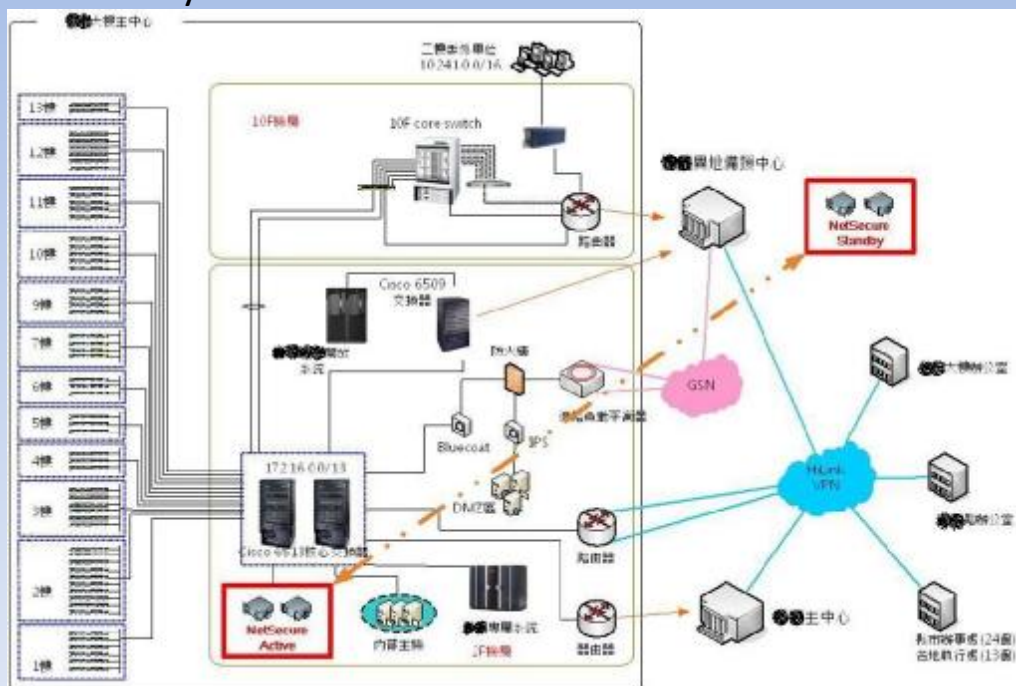
全部	显示全部	操作人姓名	操作人ID	功能名称	操作方式	操作时间
		admin	10.1.2.20	系统操作记录	删除	2006-07-13 17:34:03
		admin	10.1.2.20	系统IP地址记录	修改	2006-07-13 17:35:42
		admin	10.1.2.20	系统IP地址记录	修改	2006-07-13 17:36:29
		admin	10.1.2.20	系统IP地址记录	修改	2006-07-13 17:36:58
		admin	10.1.2.20	系统日志记录	修改	2006-07-13 17:40:25
		admin	10.1.2.20	系统IP地址记录	修改	2006-07-13 18:04:20
		admin	10.1.2.20	系统日志记录	删除	2006-07-13 18:04:41
		admin	10.1.2.20	系统IP地址记录	修改	2006-07-13 18:04:49
		admin	10.1.2.20	系统日志记录	删除	2006-07-13 18:06:16


 前1页 | 上1页 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... | 下1页 | 后1页 |
 

一休資訊科技股份有限公司

NetSecure

Case Study :



一休資訊科技股份有限公司

New Function

V 2.4.1

- NetSecure & NS Locker & NS Defender
- 全新的 NetSecure Licence 授權機制
- 提供 L2 封鎖的 Port 號資訊
- 開放 ACL 群組設定
- IP 保管人
- 新增訪客管理流程
- 更彈性的 DHCP 功能
- ...

Next Release

- DNS 黑名單管理與紀錄
- ...

一休資訊科技股份有限公司

NetSecure

功能簡介-授權



The image shows a screenshot of the NetSecure license management interface. It features a red header bar with a logo on the left and the text '歡迎使用 NetSecure' in the center. Below the header, there is a table with license information. The table has two columns: '產品序號' (Product Serial Number) and '產品啟動金鑰' (Product Activation Key). The '產品序號' column contains the value 'DE9B-8C68-FAB4-BB1E-9D53-E820-C954-6D8A'. The '產品啟動金鑰' column contains a text input field with the value '選擇檔案' (Select File) and a button labeled '匯入' (Import). Below the table, there is a section labeled '目前金鑰內容' (Current Key Content) which displays the license details: '產品: NetSecure', '授權類型: 測試版' (License Type: Trial Version), and '到期日: 2010-10-02 14:41:02' (Expiration Date: 2010-10-02 14:41:02). In the top right corner of the interface, there are links for 'EQIT首頁' (EQIT Home) and '聯絡信箱' (Contact Us).

產品序號	DE9B-8C68-FAB4-BB1E-9D53-E820-C954-6D8A
產品啟動金鑰	選擇檔案 匯入
目前金鑰內容	產品: NetSecure 授權類型: 測試版 到期日: 2010-10-02 14:41:02

一休資訊科技股份有限公司

NetSecure

功能簡介-封鎖後可通行



一休資訊科技股份有限公司

NetSecure

功能簡介-封鎖後可通行



一休資訊科技股份有限公司

NetSecure

功能簡介-IP保管人



一休資訊科技股份有限公司

NetSecure

功能簡介-訪客管理



一休資訊科技股份有限公司

NetSecure

功能簡介-訪客管理



Net Secure

系統管理 | 登錄管理 | 封鎖管理 | 線上使用說明

資料狀態: [下拉] PCNAME: [輸入] MAC: [輸入]
訪客姓名: [輸入] 證件號碼: [輸入] 最近使用IP: [輸入] [搜尋]

首頁 >> 系統管理 >> 訪客管理 >> 訪客管理查詢/查詢

資料詳見: 網頁顯示: 10頁

編號	訪客狀態	訪客/證件號碼	PCNAME	MAC	最近日期	最近時間	最近使用IP	訪客資料	新增	刪除
000_jerry	訪客	000000	00	00180e7d90e4	2010-09-08 10:00:00	2010-09-18 16:59:59	0000-00-00 00:00:00	[圖示]	[圖示]	[圖示]

* [已申請]或[刪除]資料，請使用[資料狀態]進行選擇。

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

系統管理 | 登錄管理 | 封鎖管理 | 線上使用說明

一休資訊科技股份有限公司

NetSecure

功能簡介-IP使用歷程



Net Secure

系統管理 | 登錄管理 | 封鎖管理 | 線上使用說明

歷史單位: [下拉] IP: [輸入] IP: [輸入] IP: [輸入]
MAC: [輸入] 上傳時間: [輸入] 上傳結束: [輸入]
MAC: [輸入] 下載時間: [輸入] 下載結束: [輸入]

首頁 >> 系統管理 >> IP使用歷程

資料詳見: 10頁

歷史單位	訪客/證件號碼	IP	MAC	上傳時間	下載時間
單位一	10.1.1.8	0026181a1718	2010-09-13 16:12:03		
單位一	10.1.1.1	0C16363d00cd	2010-09-13 14:09:03		2010-09-13 16:09:06
單位一	10.1.1.8	0026181a1718	2010-09-08 18:36:07		2010-09-13 16:05:09
單位一	10.1.1.15C	000c2080c685	2010-09-13 16:05:03		
單位一	10.1.1.113 /網立南	20cf302b0fc3	2010-09-13 16:02:03		
單位一	10.1.1.113 /網立南	20cf302b0fc3	2010-09-13 15:58:04		2010-09-13 15:58:07
單位一	10.1.1.113 /網立南	20cf302b0fc3	2010-09-13 08:58:03		2010-09-13 15:49:05
單位一	10.1.1.15+	0C089f9bcb0b	2010-09-13 15:20:04		
單位一	10.1.1.157	001a8057b8ee	2010-09-13 08:46:02		2010-09-13 11:59:06
單位一	10.1.1.15+	0C089f9bcb0b	2010-09-13 08:27:03		2010-09-13 11:49:06
單位一	10.1.1.15	0013d45a0066	2010-09-13 09:57:03		
單位一	169.35+69.131	001a8057b8ee	2010-09-13 08:46:02		2010-09-13 09:47:05
單位一	10.1.1.1	000c2944d779	2010-09-13 09:17:07		
單位一	10.1.1.15	485b387c0613	2010-09-13 08:44:03		
單位一	10.1.1.10.101	0816363cf1e1	2010-09-13 08:39:03		
單位一	10.1.1.1+3	20cf302b0fc3	2010-09-13 08:11:03		
單位一	10.1.1.1+3	20cf302b0fc3	2010-09-11 09:30:03		2010-09-11 13:07:04
單位一	10.1.1.223	000c2944d779	2010-09-11 04:06:03		
單位一	10.1.1.223	000c2944d779	2010-09-09 01:45:03		2010-09-11 04:04:05
單位一	10.1.1.1+3	20cf302b0fc3	2010-09-10 06:16:02		2010-09-10 22:44:05

一休資訊科技股份有限公司

NetSecure

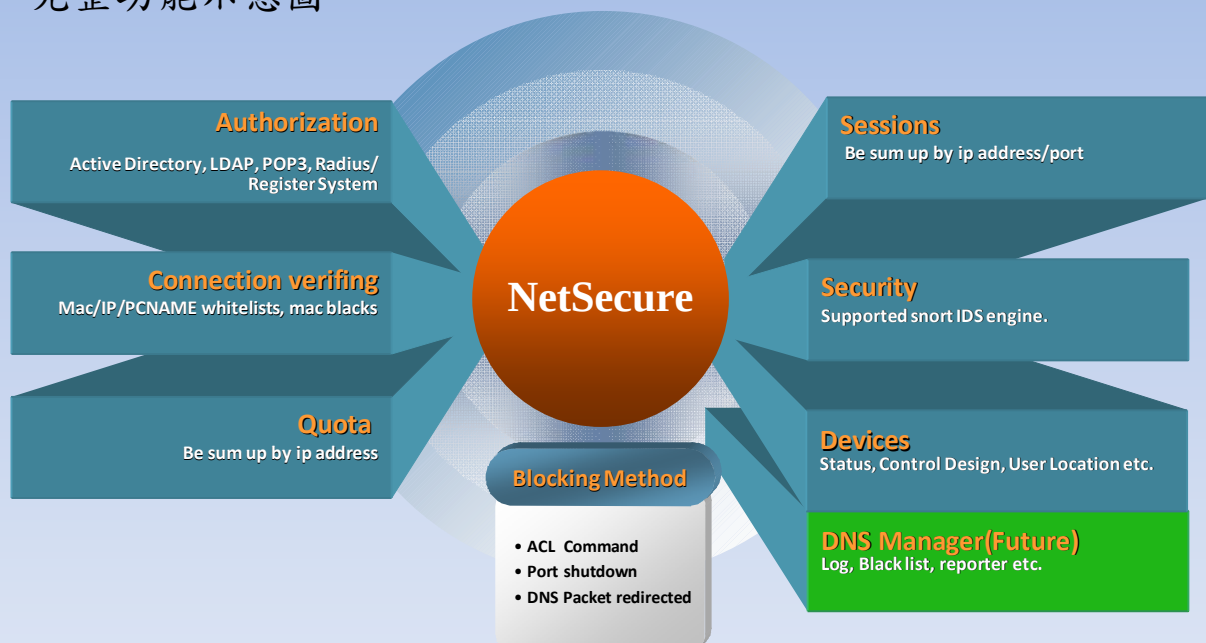
功能簡介- IPMAC 回收



一休資訊科技股份有限公司

NetSecure

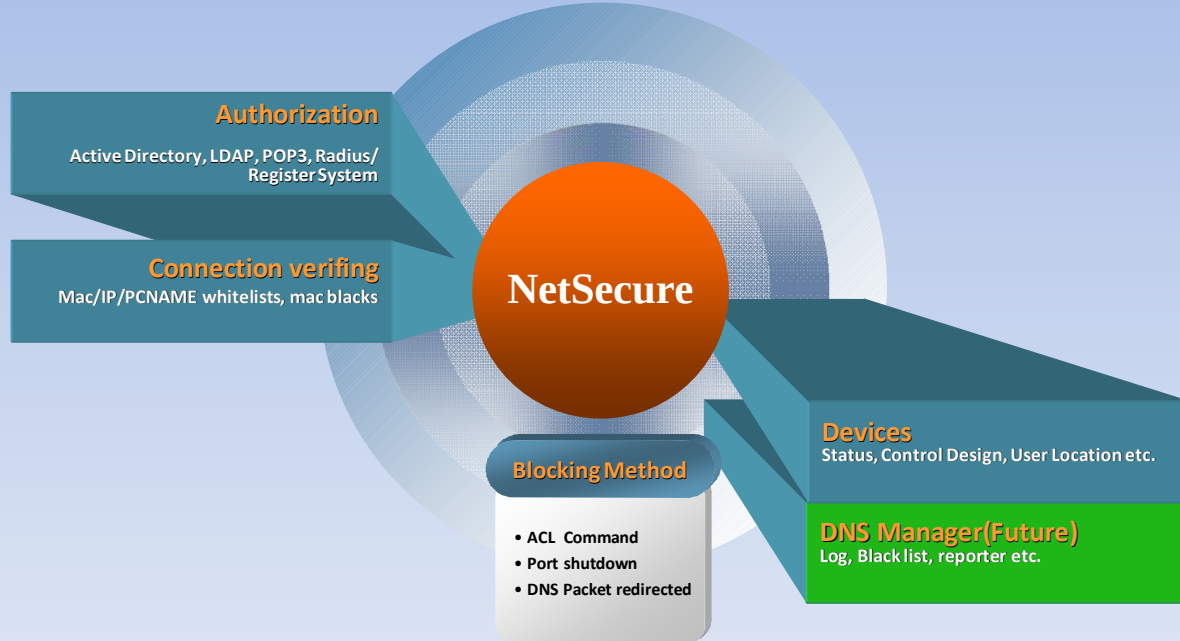
完整功能示意圖



一休資訊科技股份有限公司

NetSecure Locker

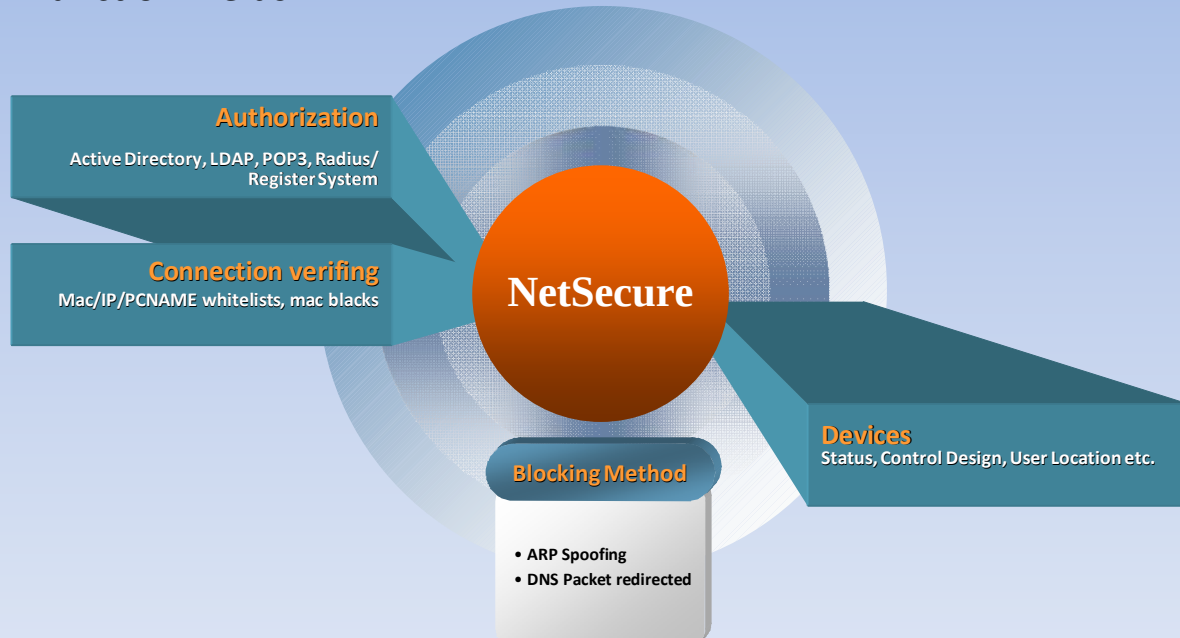
Function Fields



一休資訊科技股份有限公司

NetSecure Defender

Function Fields



一休資訊科技股份有限公司

NS Locker new function for DNS Manager

- a. DNS網域黑名單
- b. DNS網域黑名單違規記錄
- c. DNS查詢詳細記錄
- d. DNS查詢次數統計報表
- e. IP進行DNS查詢次數統計報表
- f. 匯入匯出DNS黑名單

一休資訊科技股份有限公司

DNS網域黑名單

代理主機：		網域名稱：	搜尋
首頁 >> 系統設定 >> DNS網域黑名單		資料共 [1844] 筆 總頁數共 [93] 頁	
☒	代理主機	網域名稱	備註
☐	金管會代理主機	*.facebooka.com	
☐		008.net	
☐		04080.com	
☐		0705.year.nsol.us	
☐		1.114central.com	
☐		1.verynx.cn	
☐		123music.m-music.net	
☐		126mail.oicp.net	
☐		12qwaszx.kmip.net	
☐		13591.com	
☐		140.116.37.40	
☐		140.119.46.35	
☐		151-m-netfixes.com	

可配合行政院技服中心DNS黑名單匯入清單

一休資訊科技股份有限公司

DNS網域黑名單違規記錄

代理主機: Client IP: 詢問DNS: 危險中繼網址或IP:

VLAN名稱: VLAN 網段名稱: 搜尋

◎ 首頁 >> 系統設定 >> DNS網域黑名單違規記錄 資料共 [298] 筆 總頁數共 [15] 頁

代理主機	Client IP	VLAN名稱	VLAN 網段名稱	詢問DNS	危險中繼網址或IP	訪問次數	造訪時間
金管會代理主機	10.1.14.2	綜合規劃處	Vlan14	10.1.1.1	www.facebook.com	1	2009-10-14 18:41:36
金管會代理主機	10.1.1.1			168.95.1.1	www.facebook.com	2	2009-10-14 18:41:36
金管會代理主機	10.1.1.1			168.95.1.1	www.facebook.com	2	2009-10-14 18:41:00
金管會代理主機	10.1.14.2	綜合規劃處	Vlan14	10.1.1.1	www.facebook.com	1	2009-10-14 18:41:00
金管會代理主機	10.1.1.1			168.95.1.1	www.facebook.com	2	2009-10-14 18:38:39
金管會代理主機	10.1.10.101	主委/副主委/主秘	Vlan10	10.1.1.1	zh-tw.facebook.com	1	2009-10-14 18:38:39
金管會代理主機	10.1.10.101	主委/副主委/主秘	Vlan10	10.1.1.1	www.facebook.com	1	2009-10-14 18:38:35
金管會代理主機	10.1.1.1			168.95.1.1	www.facebook.com	2	2009-10-14 18:38:35
金管會代理主機		主委/副主委/					2009-10-14

一休資訊科技股份有限公司

DNS查詢詳細記錄

代理主機: Client IP: 詢問DNS: VLAN名稱:

VLAN 網段名稱:

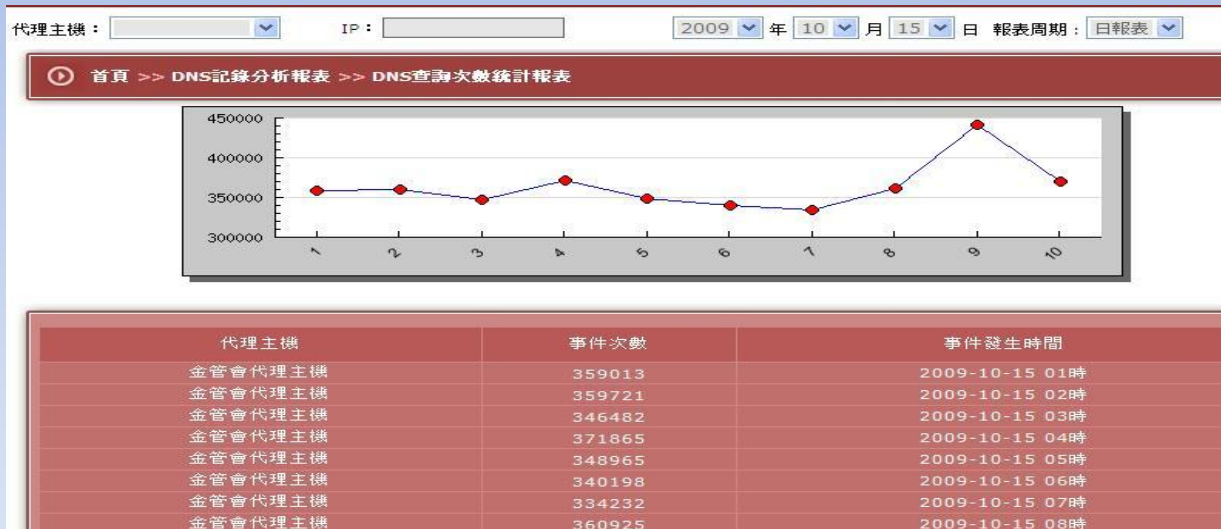
危險中繼網址或IP: 開始時間: 2009-10-15 10:40:35 結束時間: 2009-10-15 10:46 搜尋

◎ 首頁 >> 系統設定 >> DNS查詢詳細記錄 資料共 [228] 筆 總頁數共 [12] 頁

代理主機	Client IP	VLAN名稱	VLAN 網段名稱	詢問DNS	危險中繼網址或IP	訪問次數	造訪時間
金管會代理主機	10.1.10.132	主委/副主委/主秘	Vlan10	10.1.1.1	netsecure.localdomain	8	2009-10-15 10:45:13
金管會代理主機	10.1.11.34	委員+秘書	Vlan11	10.1.1.1	36.11.1.10.in-addr.arpa	4	2009-10-15 10:45:03
金管會代理主機	10.1.11.34	委員+秘書	Vlan11	10.1.1.1	36.11.1.10.in-addr.arpa	3	2009-10-15 10:45:04
金管會代理主機	10.1.15.3	國際業務處	Vlan15	10.1.1.1	docs.google.com	1	2009-10-15 10:45:09
金管會代理主機	10.1.1.1			168.95.1.1	writely.l.google.com	2	2009-10-15 10:45:09
金管會代理主機	10.1.1.249			10.1.1.1	186.1.16.172.in-addr.arpa	1	2009-10-15 10:45:10
金管會代理主機	10.1.1.249			10.1.1.1	185.1.16.172.in-addr.arpa	1	2009-10-15 10:45:10
金管會代理主機	10.1.1.1	委員+秘書	Vlan11	10.1.1.1	time.sitime.gov.tw.localdomain	1	2009-10-15

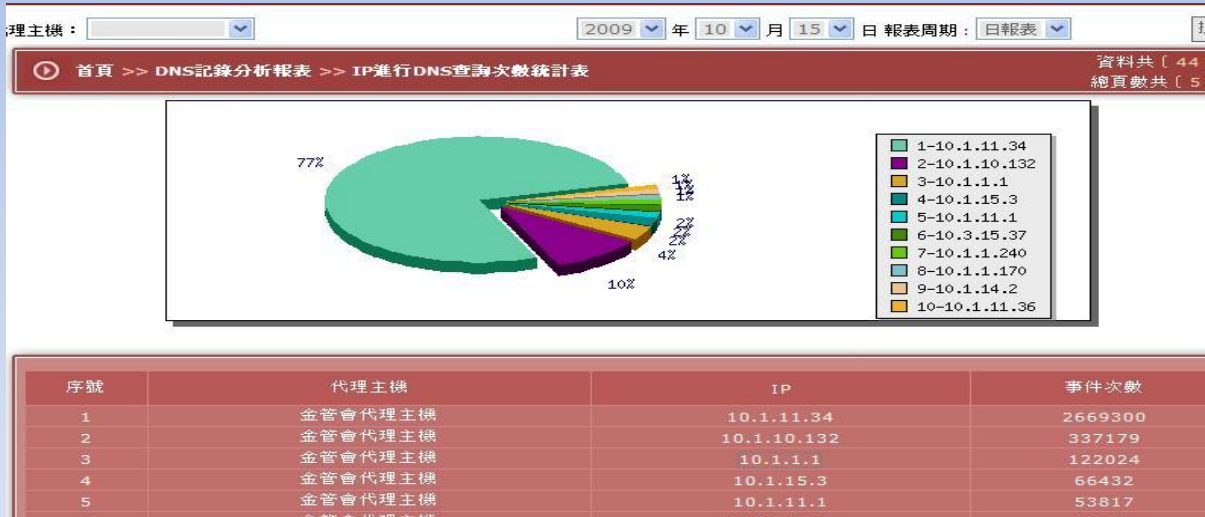
一休資訊科技股份有限公司

DNS查詢次數統計報表



一休資訊科技股份有限公司

IP進行DNS查詢次數統計報表



一休資訊科技股份有限公司

匯入匯出DNS黑名單

[首頁](#) >> [匯入及備份](#) >> [匯入匯出DNS網域黑名單](#)

上傳csv格式文檔 代理主機： 全部匯入 瀏覽... 匯入	範例說明 匯入檔案名稱：dns_block_[日期]_[時間].csv 匯入檔案欄位順序： Domain Name,備註 匯入檔案內容範例(請用逗號隔開): eqit.com.tw,memo webmail.com.tw,memo *. Domain Name欄位為空白或格式錯誤，系統將自動捨棄該筆資料!!! *. 匯入資料與目前存在資料重複時(Domain Name+Agent)，系統將自動捨棄該筆匯入資料!!! *. 全部匯入意指將此次匯入資料同時派送到每台Agent主機，如否，請選擇要匯入的代理主機!!!
匯出csv格式文檔 代理主機： 全部匯出 匯出	範例說明 匯出檔案名稱：dns_block_[日期]_[時間].csv 匯出檔案欄位順序： Domain Name,備註,代理主機名稱 *. 全部匯出意指將每台Agent主機資料集中進行匯出，如否，請選擇要匯出的代理主機!!!

一休資訊科技股份有限公司

阻擋網路應用



一休資訊科技股份有限公司

NetSecure

Thank You

一休資訊科技股份有限公司