FortiNAC -

讓你內網 IoT 無所遁形且可管理

2021

Dave Peng 彭冠嘉

Fortinet 台灣區技術顧問

Agenda

1. 論 IoT 辨識的重要性
2. 有了 FortiNAC，萬事 OK
3. FortiNAC Demo

201705

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

201908

微軟：俄國駭客使用IoT裝置入侵企業網路

曾經攻擊過美國民主黨、奧林匹克委員會，以VPN Filter惡意程式大規模感染路由器的國家級駭客組織APT 28，近期被發現企圖利用VoIP電話、印表機及影片解碼裝置，駭入特定企業網路

202001

研究人員踢爆GE Medical醫療裝置含有重大安全漏洞，將允許駭客關閉監護裝置

GE Medical的醫療裝置內含6大安全漏洞，成功的開採將允許駭客關閉監護裝置、變更警報設定，或是自遠端控制相關裝置，目前GE Medical尚未完成修補作業，僅提供用戶暫時緩解方法

快速套用模組 ---- 弱點

不熟網路資安 ---- 不該突破

現有產品底層 ---- 錯誤小眾

72

裝置 & 儀器並不安全

69

裝置 & 儀器使用
應用程式並不安全

90

超過一種手持裝置

76

醫院大量使用手持裝置 / BYOD

646 Million

IoT 設備會被採用

Agenda

1. 論 IoT 辨識的重要性
2. 有了 FortiNAC，萬事 OK
3. FortiNAC Demo

FortiNAC

看不到，則防不到

看透

控管

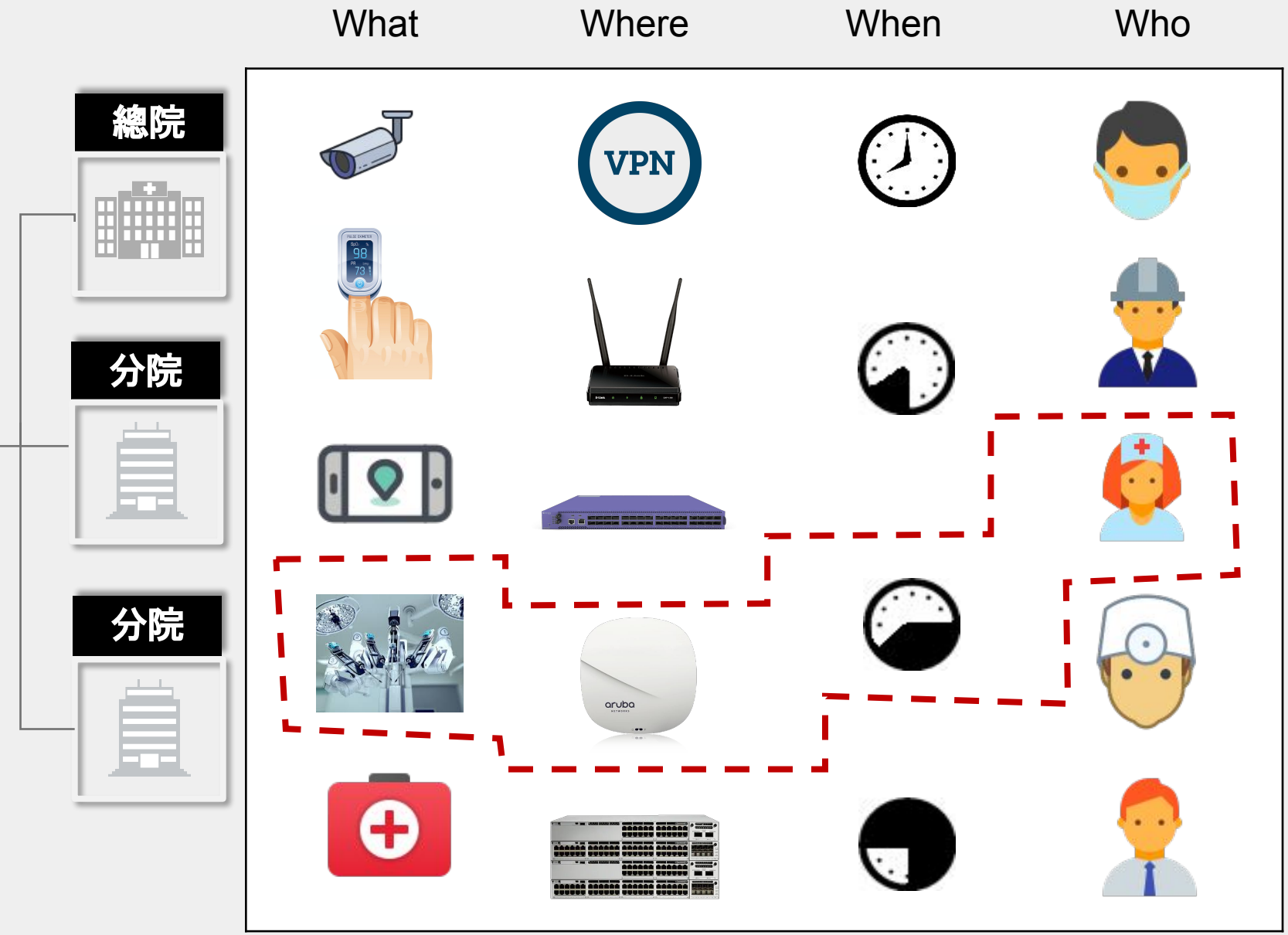
自動化

IoT

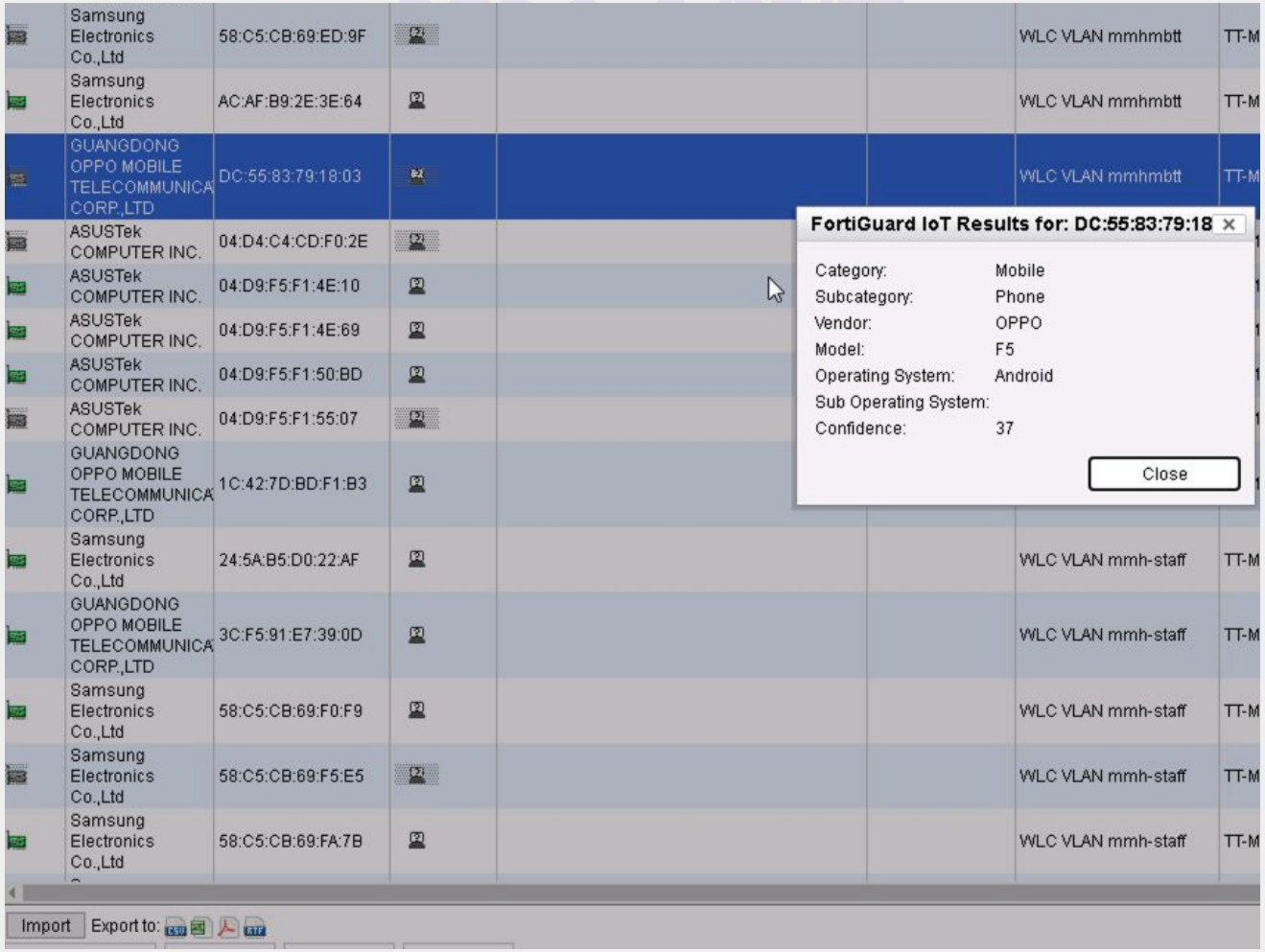
自動化辨識

NAC

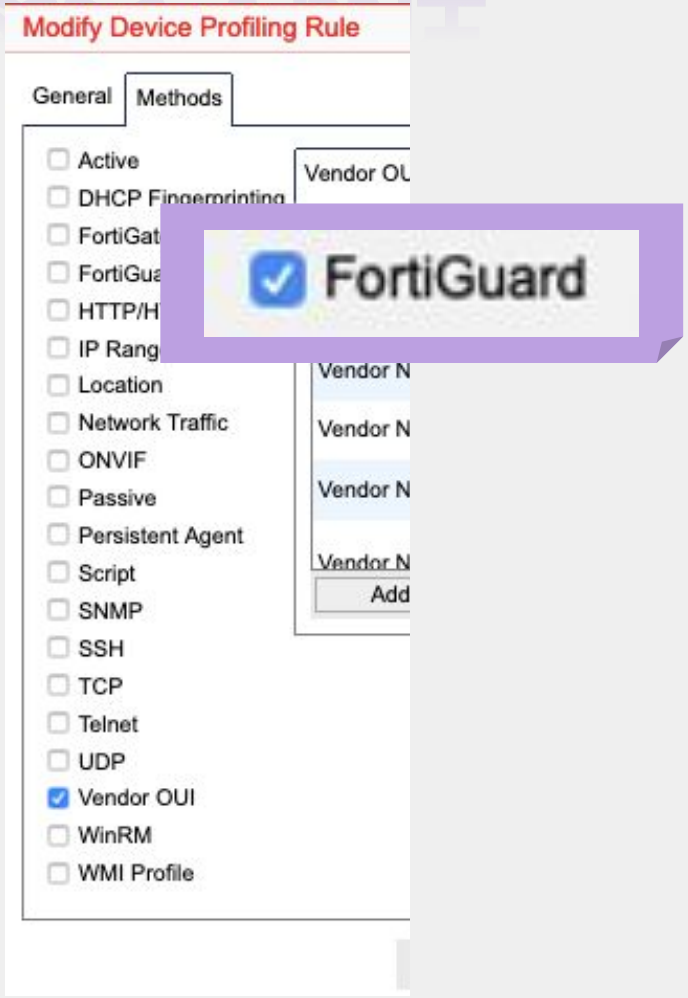
零信任控管



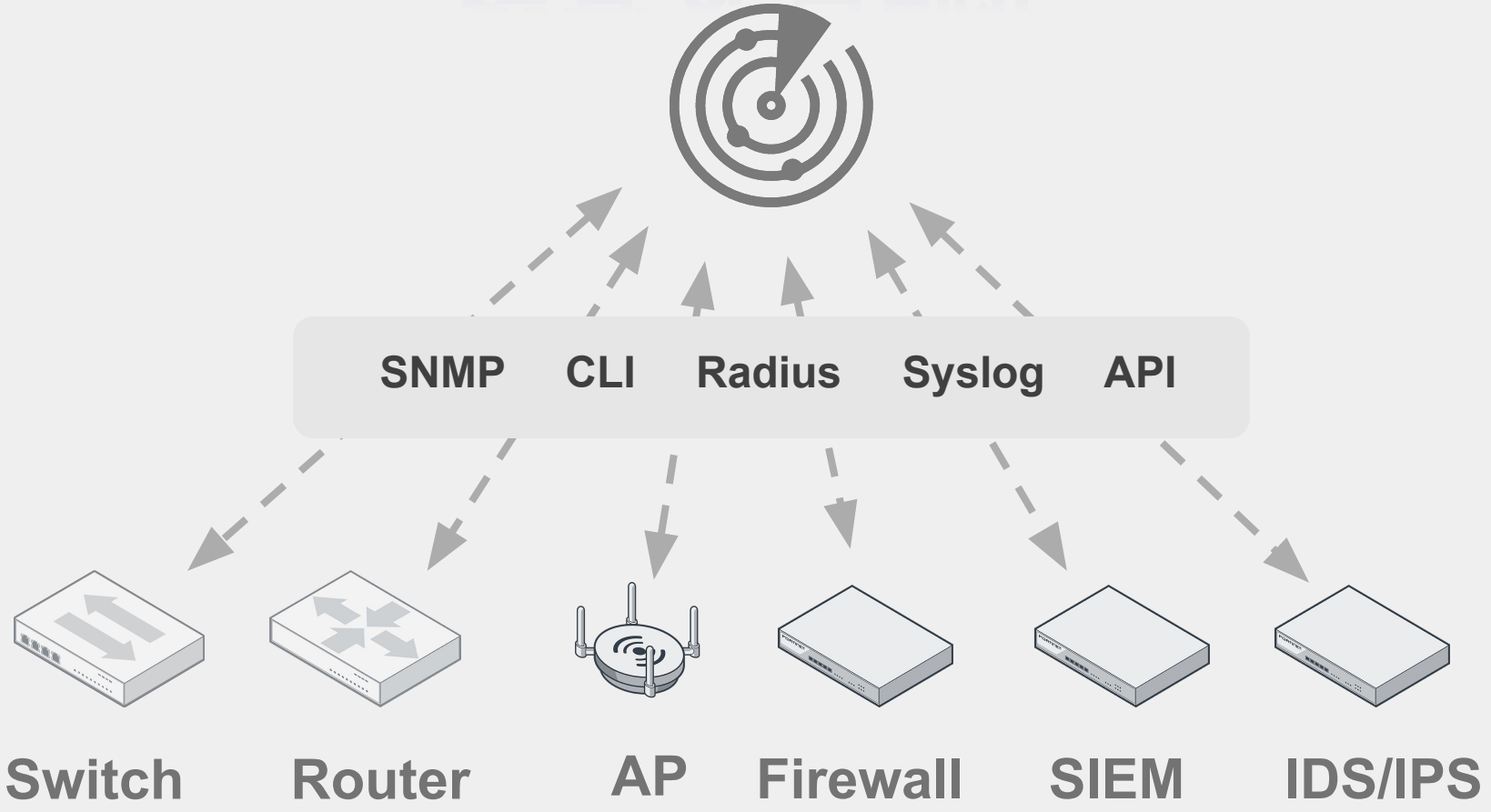
先天可視性



後天可視性



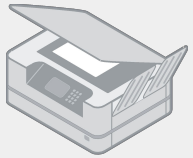
控管 & 自動化



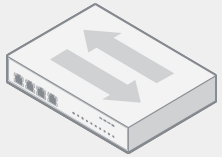
Support Devices

FortiNAC 註冊&辨識機制

自動化辨識

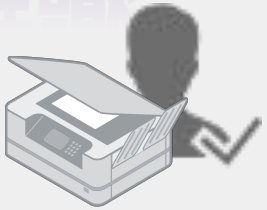


印表機進入



Switch 通知 FortiNAC
印表機 MAC

FortiNAC 辨識為印表機

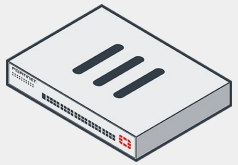


FortiNAC 售予權限

FortiNAC 第一時間阻絕病毒

自動化隔離

病原體進入內網

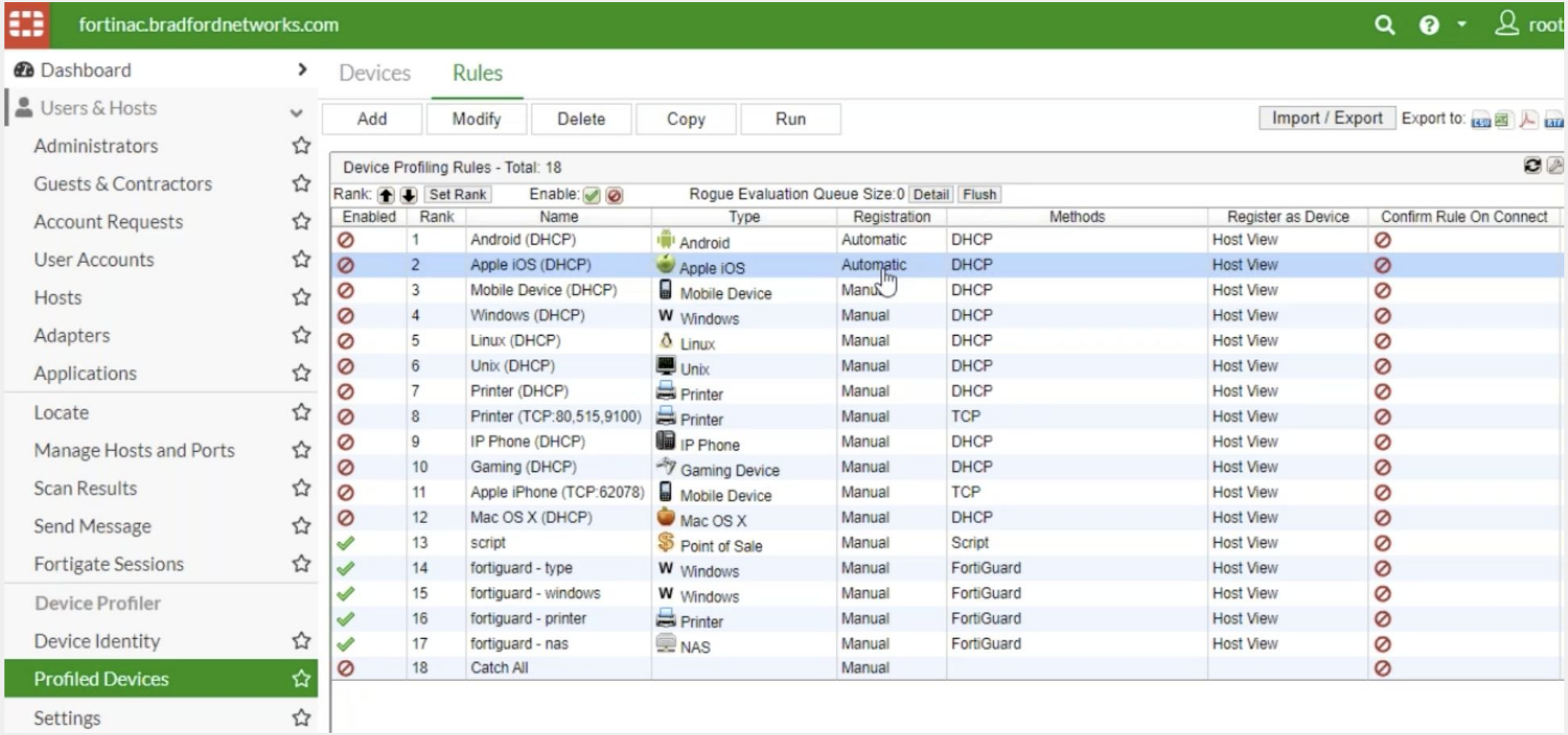


防火牆發現問題

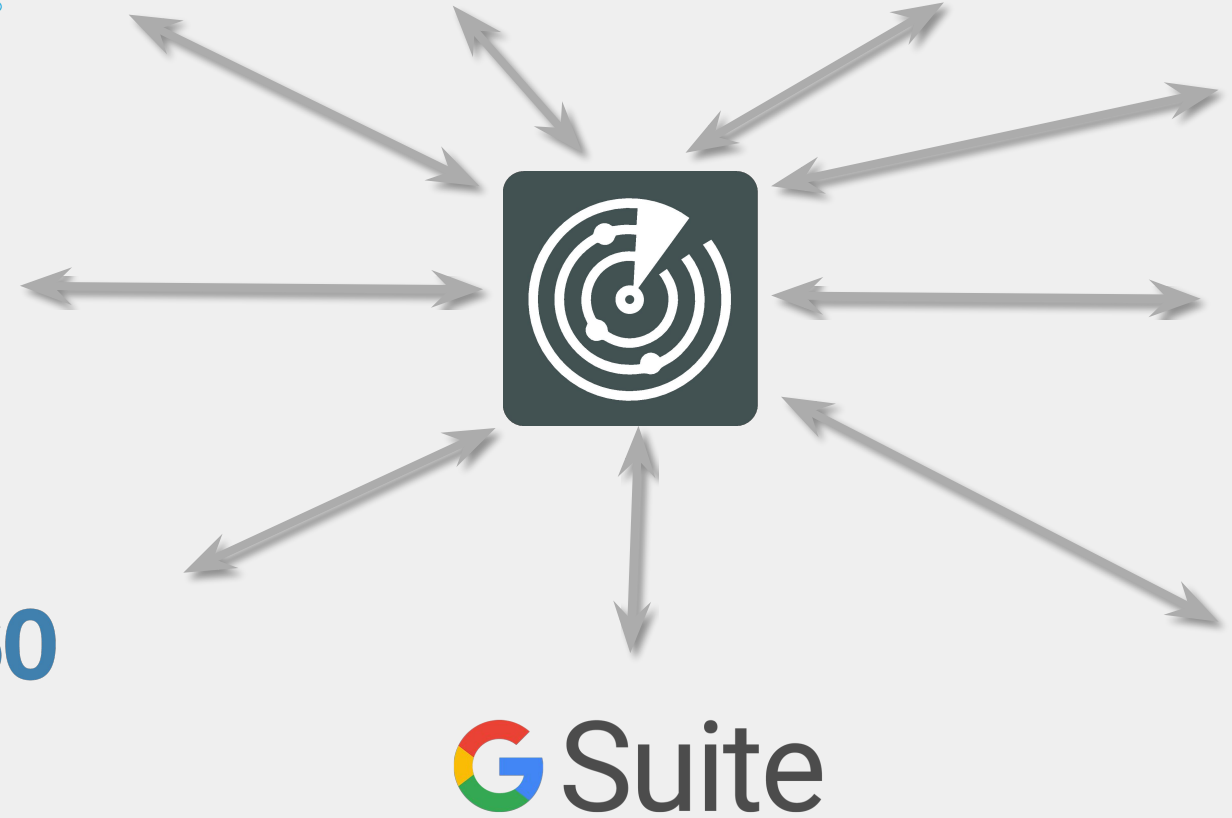
FortiNAC 將其阻擋在
Switch port

成功隔離病毒

簡單明瞭的辨識 policy



FortiNAC Connector



airwatch by vmware

Microsoft Intune

CITRIX

jamf

MobileIron

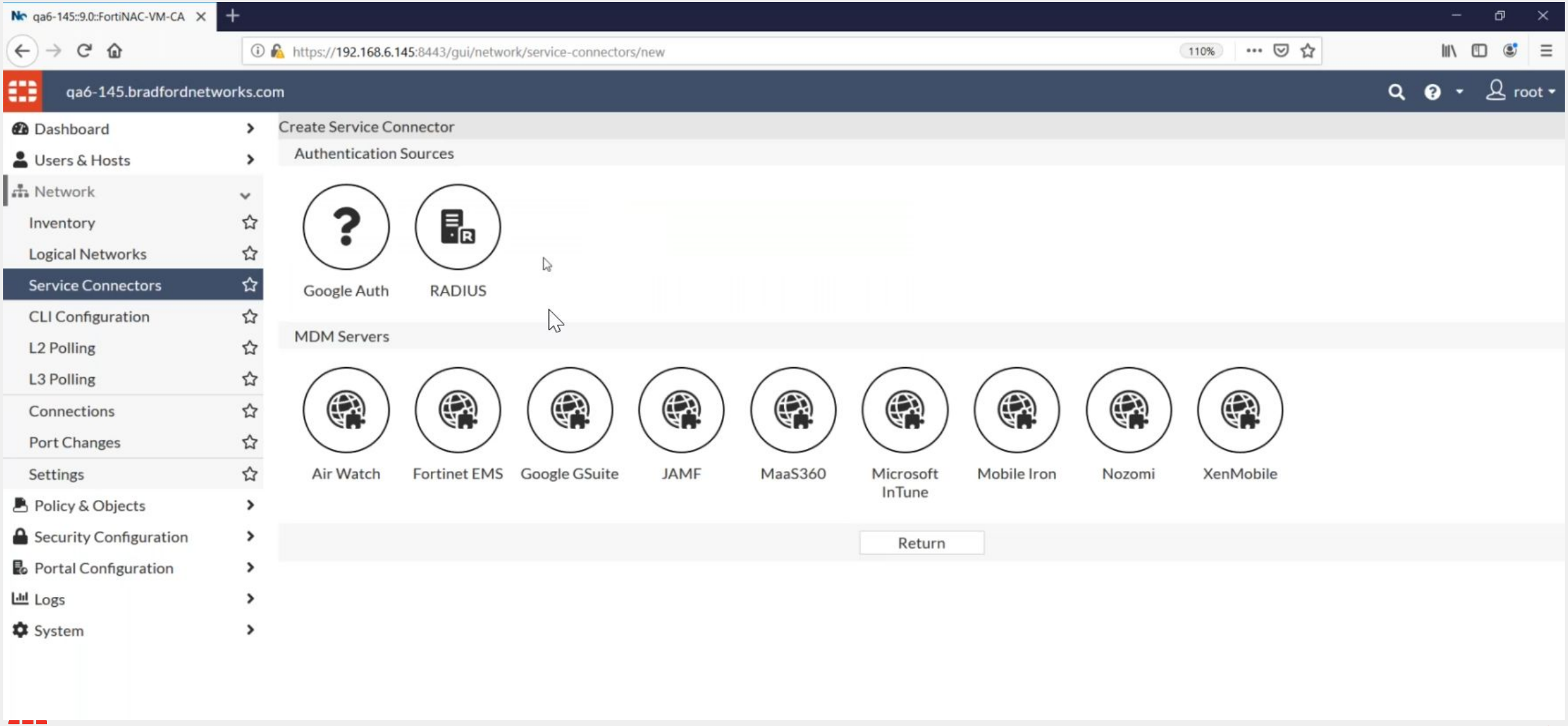
NOZOMI NETWORKS

IBM MaaS360

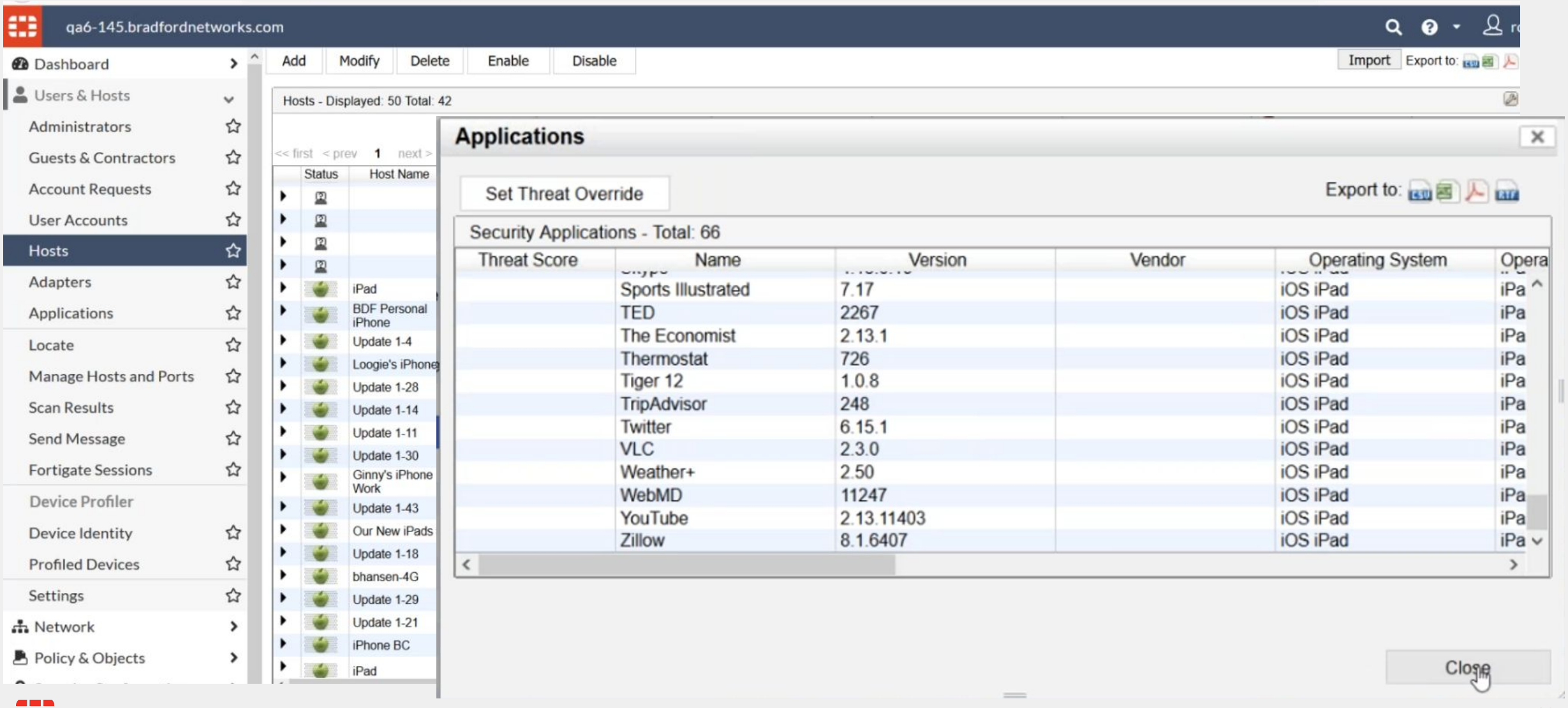
G Suite

FORTINET

FortiNAC Connector



FortiNAC Connector - JAMF

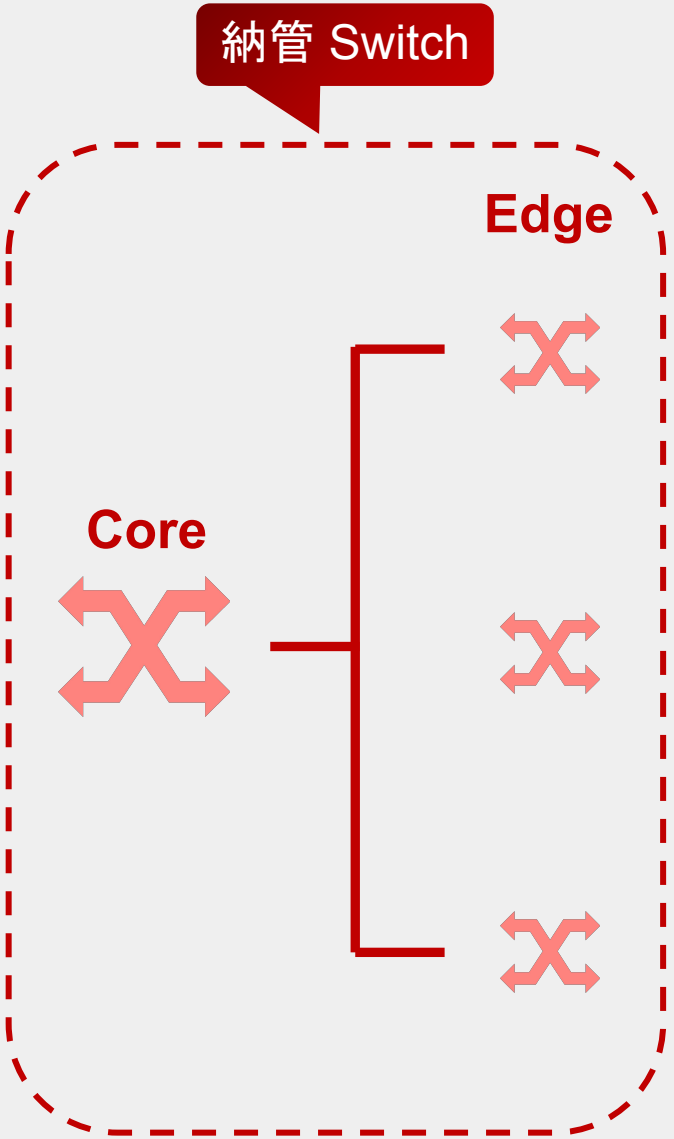


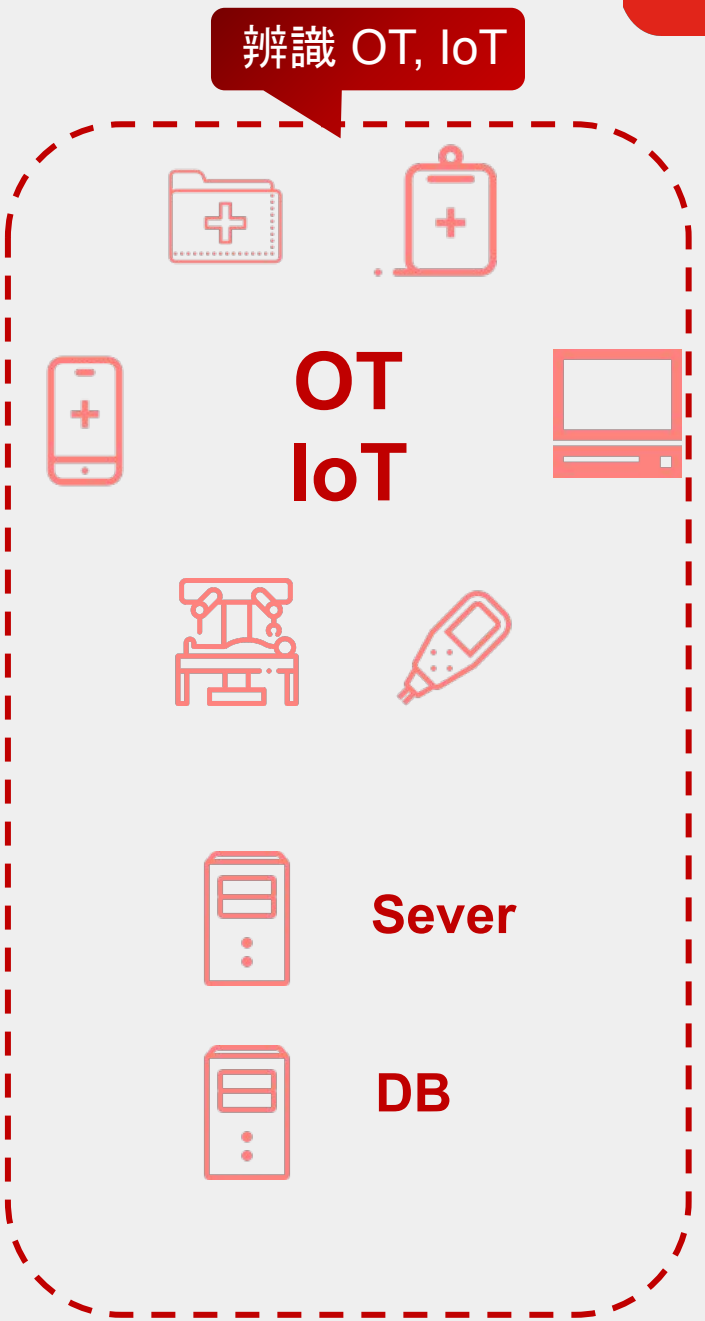
Agenda

1. 論 IoT 辨識的重要性
2. 有了 FortiNAC，萬事 OK
3. FortiNAC Demo

架構

FortiNAC





MIC 設備

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	HUAWEI TECHNOLOGIES CO.,LTD	24:31:54:F8:7C:52		WLC VLAN ncjs-ap	TT-MMH		ncjs-ap	Android Tablet Android	12/23/20 10:26 AM GMT+0800	01/18/21 01:13 PM GMT+0800
	HUAWEI TECHNOLOGIES CO.,LTD	F4:63:1F:CD:3C:17		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/24/20 09:58 AM GMT+0800	01/18/21 09:49 AM GMT+0800
	HUAWEI TECHNOLOGIES CO.,LTD	F4:BF:80:B7:5B:17		WLC VLAN mmh-staff	TT-MMH		mmh-staff		01/18/21 03:35 PM GMT+0800	01/18/21 04:26 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Xiaomi Communications Co Ltd	20:47:DA:2A:C6:97		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	01/02/21 08:02 PM GMT+0800	01/18/21 04:56 PM GMT+0800
	Xiaomi Communications Co Ltd	EC:D0:9F:38:B4:0A		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/25/20 09:43 AM GMT+0800	01/18/21 04:46 PM GMT+0800
	Xiaomi Communications Co Ltd	F4:F5:DB:CB:0B:E7		WLC VLAN mmh-guest	TT-MMH		mmh-guest		01/17/21 03:11 PM GMT+0800	01/17/21 03:31 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shenzhen TINNO Mobile Technology Corp.	B4:39:39:18:15:37		WLC VLAN mmh-staff	TT-MMH		mmh-staff	Android Phone Android	12/21/20 05:56 PM GMT+0800	01/04/21 08:50 PM GMT+0800	01/18/21 08:50 PM GMT+0800
	Shenzhen TINNO Mobile Technology Corp.	BC:41:01:F7:37:23		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/24/20 09:57 AM GMT+0800	01/16/21 03:48 PM GMT+0800	
	Shenzhen TINNO Mobile Technology Corp.	44:D3:AD:D8:F0:DD		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/25/20 08:01 AM GMT+0800	12/25/20 02:27 PM GMT+0800	

MIC 設備

HUAQIN 华勤通讯

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shanghai Huaqin Telecom Technology Co.,Ltd	90:21:81:F6:30:5B		WLC VLAN mmh-staff	TT-MMH		mmh-staff		12/29/20 05:14 PM GMT+0800	01/11/21 05:32 PM GMT+0800	01/25/21 05:32 PM GMT+0800

HIKVISION

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Hangzhou Hikvision Digital Technology Co.,Ltd.	28:57:BE:84:F4:CB		A-tt-5f-c2960-1-50 Gi0/18 { DVR_IDF }	TT-MMH		10	Network NAS	12/21/20 05:16 PM GMT+0800	12/21/20 05:16 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shenzhen Geniatech Inc, Ltd	AC:DB:DA:52:C7:AF		A-tt-2f-c2960-2-24 Gi2/0/34 { A2322 }	TT-MMH	FortiGuard-Moblie-Device-2	226	Mobile Device Android Phone Android	12/21/20 05:38 PM GMT+0800	01/05/21 11:15 AM GMT+0800	
	Shenzhen Geniatech Inc, Ltd	AC:DB:DA:54:6D:A8		A-tt-2f-c2960-2-24 Gi2/0/35 { A2323 }	TT-MMH		226	Cable Box Android	12/22/20 09:19 AM GMT+0800	01/18/21 04:08 PM GMT+0800	02/01/21 04:08 PM GMT+0800

上海天奕达电子科技有限公司

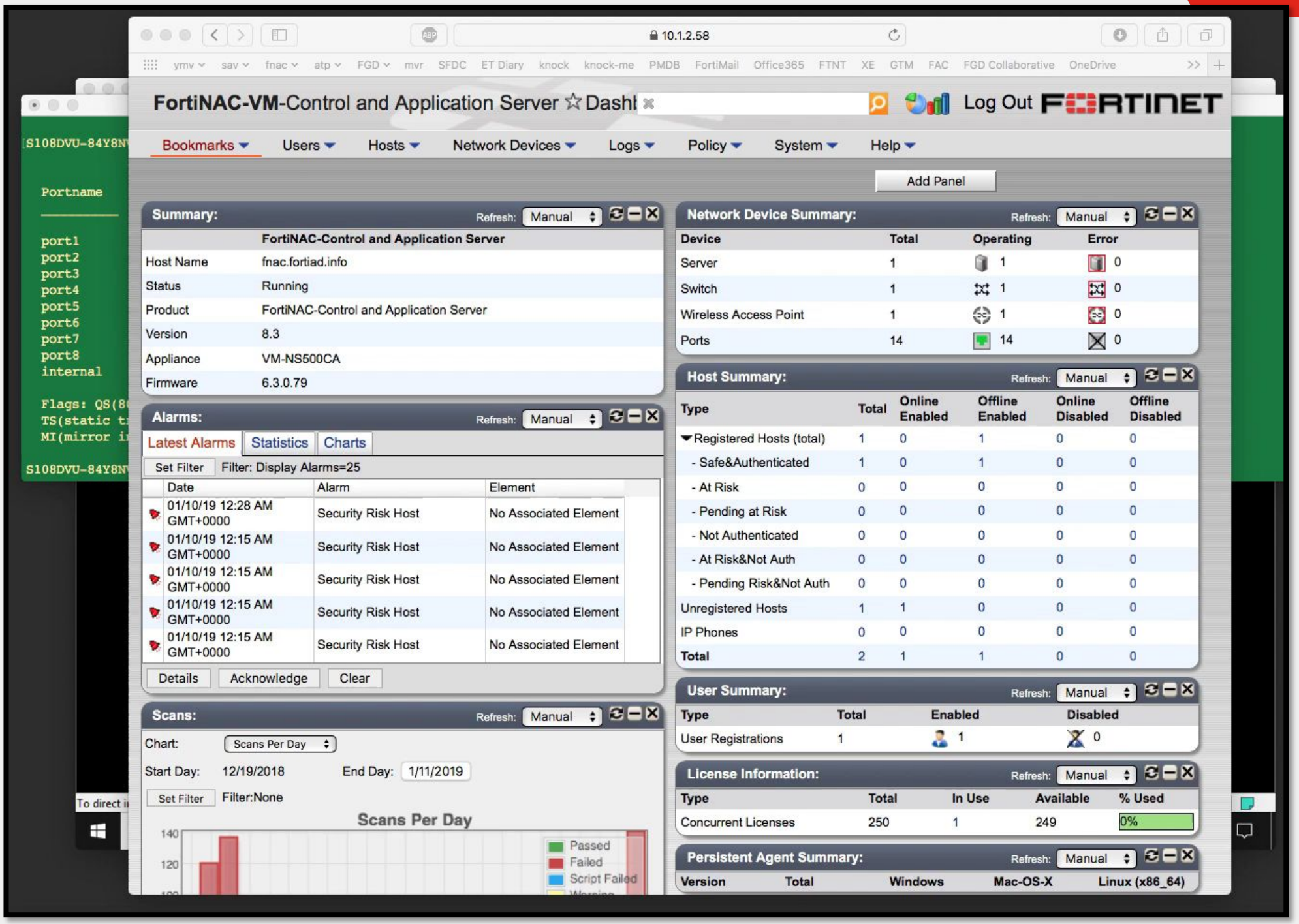
上海天奕达（TYD）电子科技有限公司是一家集研发、设计、服务为一体的现代化高新技术企业，专业从事智能手持、智能穿戴、物联网IOT等产品的开发与服务。

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Shanghai TYD Elecronic Technology Co. Ltd	C8:AE:9C:D4:81:8B		WLC VLAN mmh-staff	TT-MMH	FortiGuard-Android	mmh-staff	Android Phone Android	12/29/20 09:57 AM GMT+0800	01/18/21 05:27 PM GMT+0800
	Shanghai TYD Elecronic Technology Co. Ltd	C8:AE:9C:D4:F3:3C		WLC VLAN mmh-guest	TT-MMH		mmh-guest		01/13/21 02:26 PM GMT+0800	01/13/21 07:31 PM GMT+0800

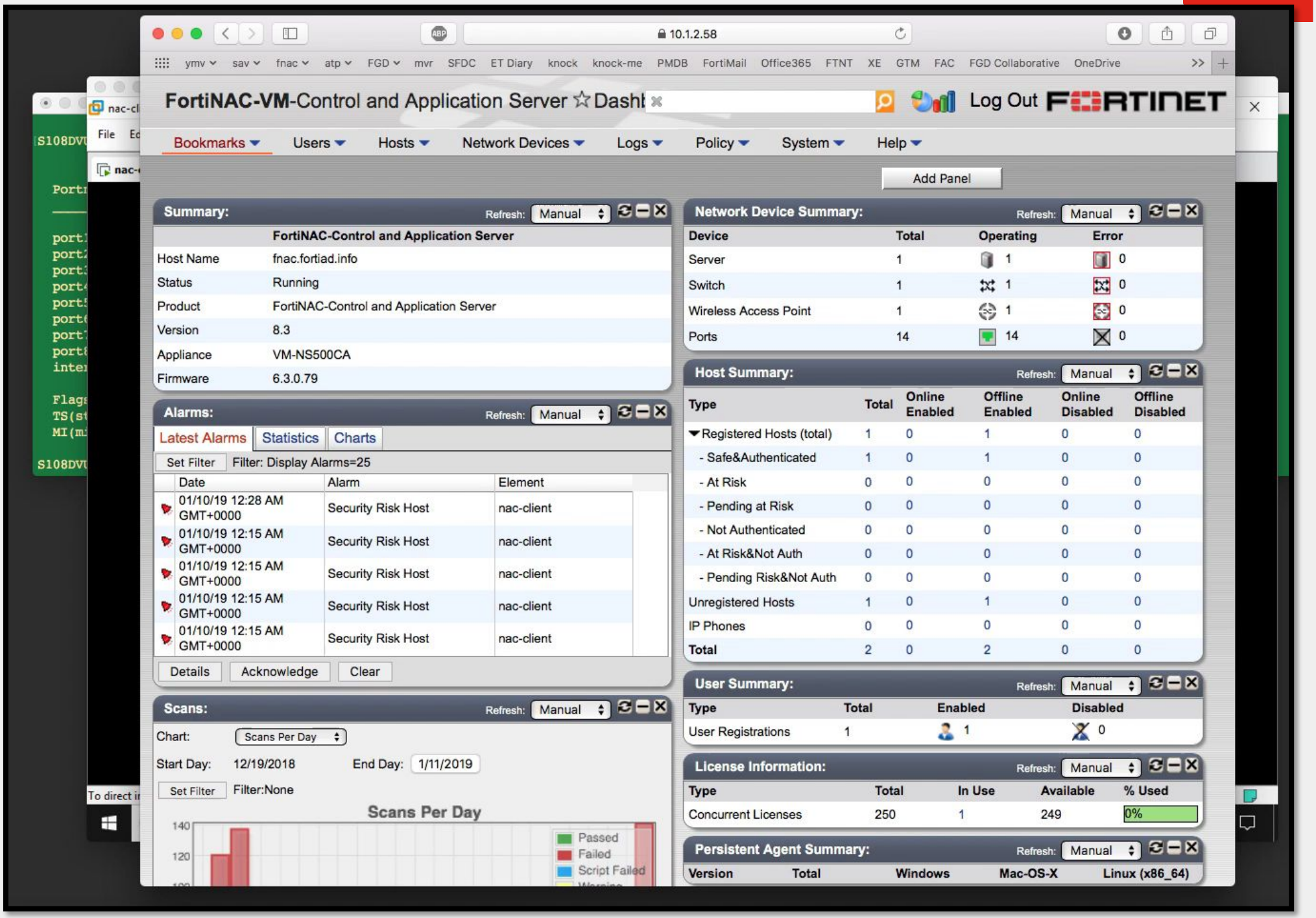
<< first < prev 1 next > last >> 100

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Zhejiang Dahua Technology Co., Ltd.	90:02:A9:B0:E0:BB		B-tt-b1f-c2960-1-10 Gi1/0/14	TT-MMH	FortiGuard-IPCam	10	Camera IP Camera	12/21/20 05:28 PM GMT+0800	01/07/21 06:26 PM GMT+0800
	Zhejiang Dahua Technology Co., Ltd.	90:02:A9:B0:E0:B6		B-tt-5f-c2960-1-5 Gi1/0/10	TT-MMH	FortiGuard-IPCam	10	Camera IP Camera	12/21/20 05:28 PM GMT+0800	12/21/20 05:18 PM GMT+0800

自動化辨識&管理


10.1.2.58
FortiNAC-VM-Control and Application Server
Log Out
FORTINET
Bookmarks
Users
Hosts
Network Devices
Logs
Policy
System
Help
Add Panel
Summary:
FortiNAC-Control and Application Server
Host Name fnac.fortiad.info
Status Running
Product FortiNAC-Control and Application Server
Version 8.3
Appliance VM-NS500CA
Firmware 6.3.0.79
Alarms:
Latest Alarms
Statistics
Charts
Set Filter
Filter: Display Alarms=25
Date
Alarm
Element
01/10/19 12:28 AM GMT+0000 Security Risk Host No Associated Element
01/10/19 12:15 AM GMT+0000 Security Risk Host No Associated Element
01/10/19 12:15 AM GMT+0000 Security Risk Host No Associated Element
01/10/19 12:15 AM GMT+0000 Security Risk Host No Associated Element
01/10/19 12:15 AM GMT+0000 Security Risk Host No Associated Element
Details
Acknowledge
Clear
Scans:
Chart: Scans Per Day
Start Day: 12/19/2018
End Day: 1/11/2019
Set Filter
Filter:None
Scans Per Day
140
120
Passed
Failed
Script Failed
Network Device Summary:
Device Total Operating Error
Server 1 1 0
Switch 1 1 0
Wireless Access Point 1 1 0
Ports 14 14 0
Host Summary:
Type Total Online Enabled Offline Enabled Online Disabled Offline Disabled
Registered Hosts (total) 1 0 1 0 0
- Safe&Authenticated 1 0 1 0 0
- At Risk 0 0 0 0 0
- Pending at Risk 0 0 0 0 0
- Not Authenticated 0 0 0 0 0
- At Risk&Not Auth 0 0 0 0 0
- Pending Risk&Not Auth 0 0 0 0 0
Unregistered Hosts 1 1 0 0 0
IP Phones 0 0 0 0 0
Total 2 1 1 0 0
User Summary:
Type Total Enabled Disabled
User Registrations 1 1 0
License Information:
Type Total In Use Available % Used
Concurrent Licenses 250 1 249 0%
Persistent Agent Summary:
Version Total Windows Mac-OS-X Linux (x86_64)
Refresh: Manual

非資產之隔離


10.1.2.58
FortiNAC-VM-Control and Application Server
Log Out
FORTINET
Bookmarks
Users
Hosts
Network Devices
Logs
Policy
System
Help
Add Panel
Summary:
Refresh: Manual
FortiNAC-Control and Application Server
Host Name fnac.fortiad.info
Status Running
Product FortiNAC-Control and Application Server
Version 8.3
Appliance VM-NS500CA
Firmware 6.3.0.79
Alarms:
Refresh: Manual
Latest Alarms
Statistics
Charts
Set Filter
Filter: Display Alarms=25
Date
Alarm
Element
01/10/19 12:28 AM GMT+0000
Security Risk Host
nac-client
01/10/19 12:15 AM GMT+0000
Security Risk Host
nac-client
01/10/19 12:15 AM GMT+0000
Security Risk Host
nac-client
01/10/19 12:15 AM GMT+0000
Security Risk Host
nac-client
01/10/19 12:15 AM GMT+0000
Security Risk Host
nac-client
Details
Acknowledge
Clear
Scans:
Refresh: Manual
Chart: Scans Per Day
Start Day: 12/19/2018
End Day: 1/11/2019
Set Filter
Filter:None
Scans Per Day
140
120
Passed
Failed
Script Failed
Network Device Summary:
Refresh: Manual
Device
Total
Operating
Error
Server 1 1 0
Switch 1 1 0
Wireless Access Point 1 1 0
Ports 14 14 0
Host Summary:
Refresh: Manual
Type
Total
Online Enabled
Offline Enabled
Online Disabled
Offline Disabled
Registered Hosts (total) 1 0 1 0 0
- Safe&Authenticated 1 0 1 0 0
- At Risk 0 0 0 0 0
- Pending at Risk 0 0 0 0 0
- Not Authenticated 0 0 0 0 0
- At Risk&Not Auth 0 0 0 0 0
- Pending Risk&Not Auth 0 0 0 0 0
Unregistered Hosts 1 0 1 0 0
IP Phones 0 0 0 0 0
Total 2 0 2 0 0
User Summary:
Refresh: Manual
Type
Total
Enabled
Disabled
User Registrations 1 1 0
License Information:
Refresh: Manual
Type
Total
In Use
Available
% Used
Concurrent Licenses 250 1 249 0%
Persistent Agent Summary:
Refresh: Manual
Version
Total
Windows
Mac-OS-X
Linux (x86_64)


FORTINET