FORTINET

THE POWER IN NETWORK PROTECTION

校園資訊安全之威脅與因應

劉乙 Jim Liu
Technical Director
Fortinet.Taiwan
0912214906
jimliu@fortinet.com

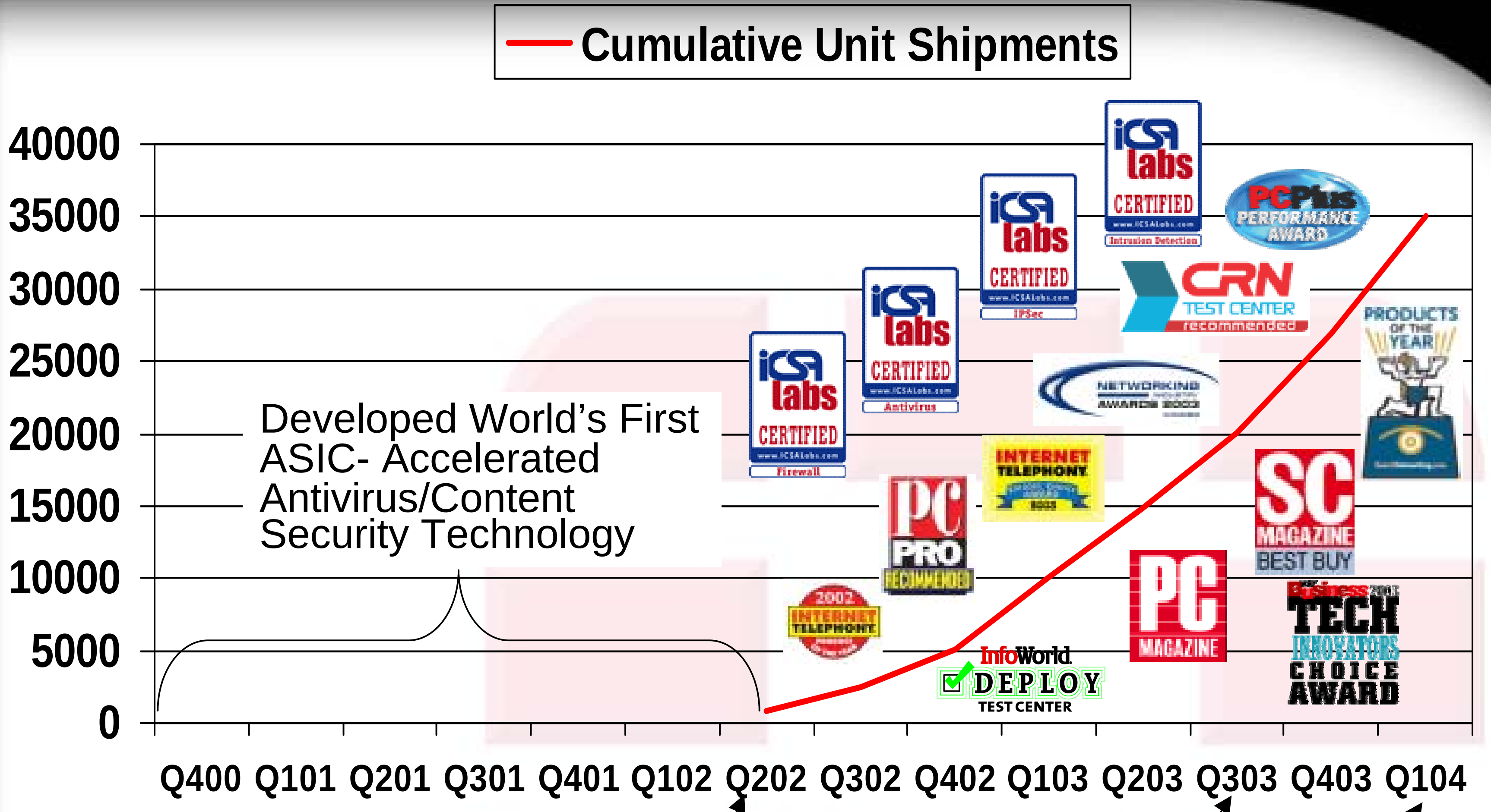
Agenda

- Fortinet 簡介
- 資訊網路潛在威脅之探討分析
- ASIC Base防毒防駭即時防護系統
- 網路安全報表統計與分析工具

THE POWER IN NETWORK PROTECTION

Fortinet 簡介 ---
Who is Fortinet？

A History of Rapid Growth and Achievement



Developed World's First ASIC- Accelerated Antivirus/Content Security Technology

Fortinet Founded

FortiGate Family Introduced

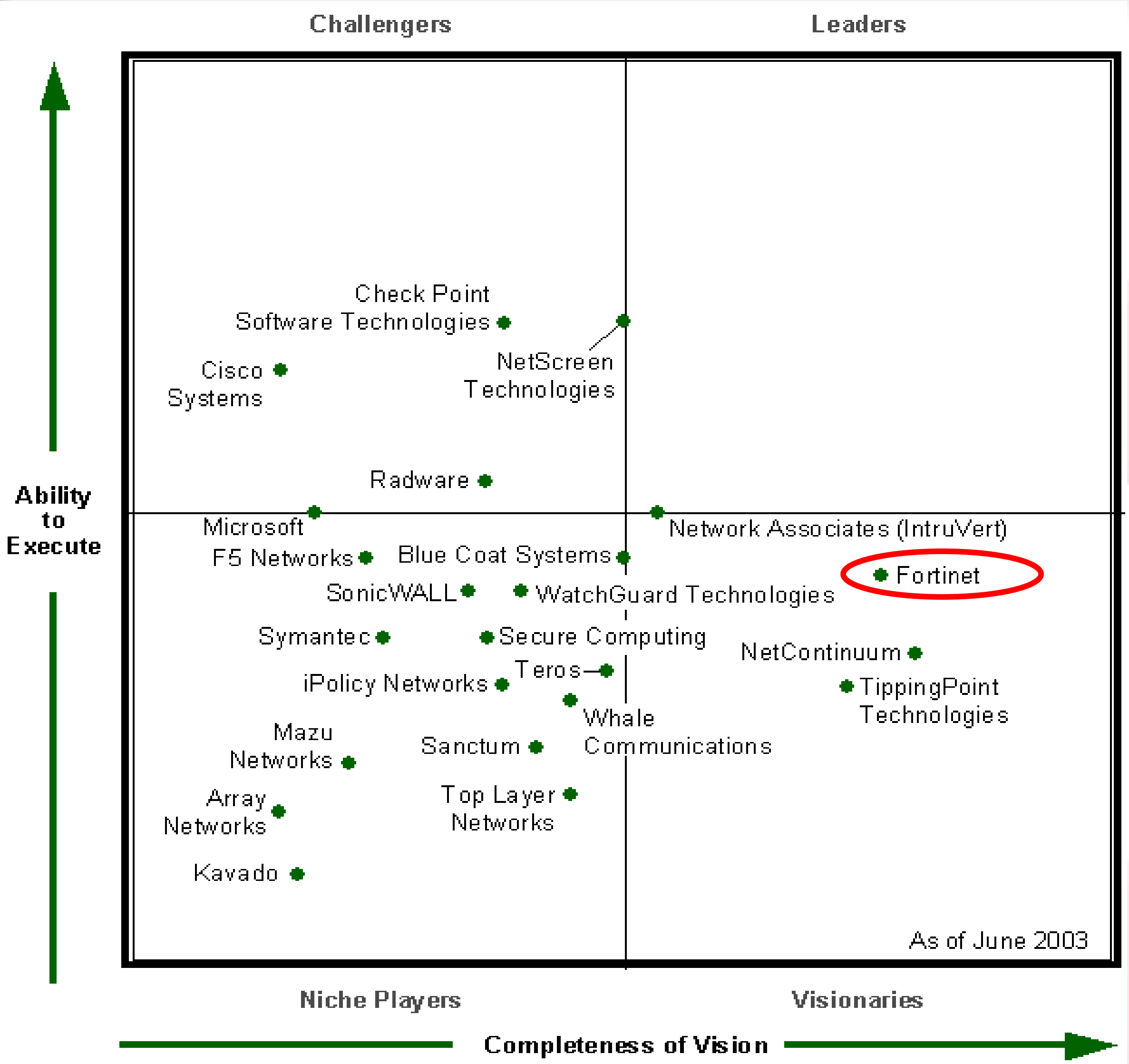
Recognized by Gartner as Visionary

$50 Million Financing

Fortinet Company Overview

- Founded October, 2000 by Ken Xie
  - Founder, former Pres. & CEO of NetScreen (NASDAQ: NSCN)
- Over 350 employees; HQ in Sunnyvale, CA
  - Offices throughout Americas, Asia, and EMEA
  - **Tokyo, Seoul, Beijing, Shanghai, Hong Kong, Taipei, Singapore, KL, Melbourne, etc.**
  - **Belgium, France, Germany, Italy, Sweden, UK**
- Creators of world’s only ASIC-powered antivirus systems
  - Addressing the need for real-time network protection
- Achieved >10x revenue growth in 2003 vs. 2002
  - Over 50,000 units shipped in under 2 and half of years
- Completed $50 million mezzanine financing Feb 2004
  - Positioned for continued rapid growth

Fortinet is Driving a Major Shift in the Evolving Security Market



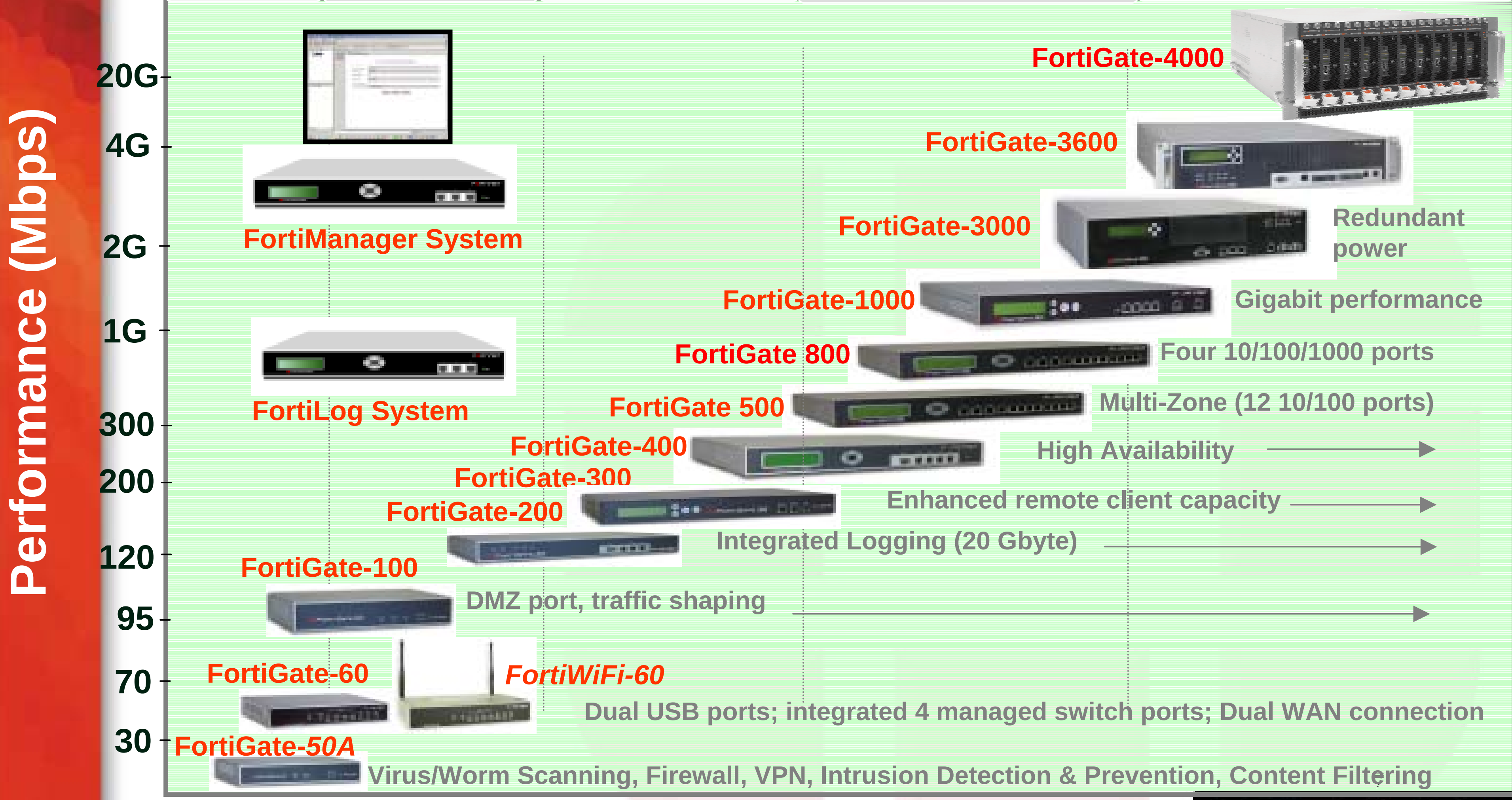
Gartner

"…Firewalls must provide a wider range of intrusion prevention capabilities, or face extinction…"

"Fortinet has demonstrated its investment in powerful network processing technology by filtering viruses in-line, which requires an unprecedented level of packet assembly and filtering."

The FortiGate Family Scales from SOHO to Service Provider

FortiGate Product Family



Capabilities

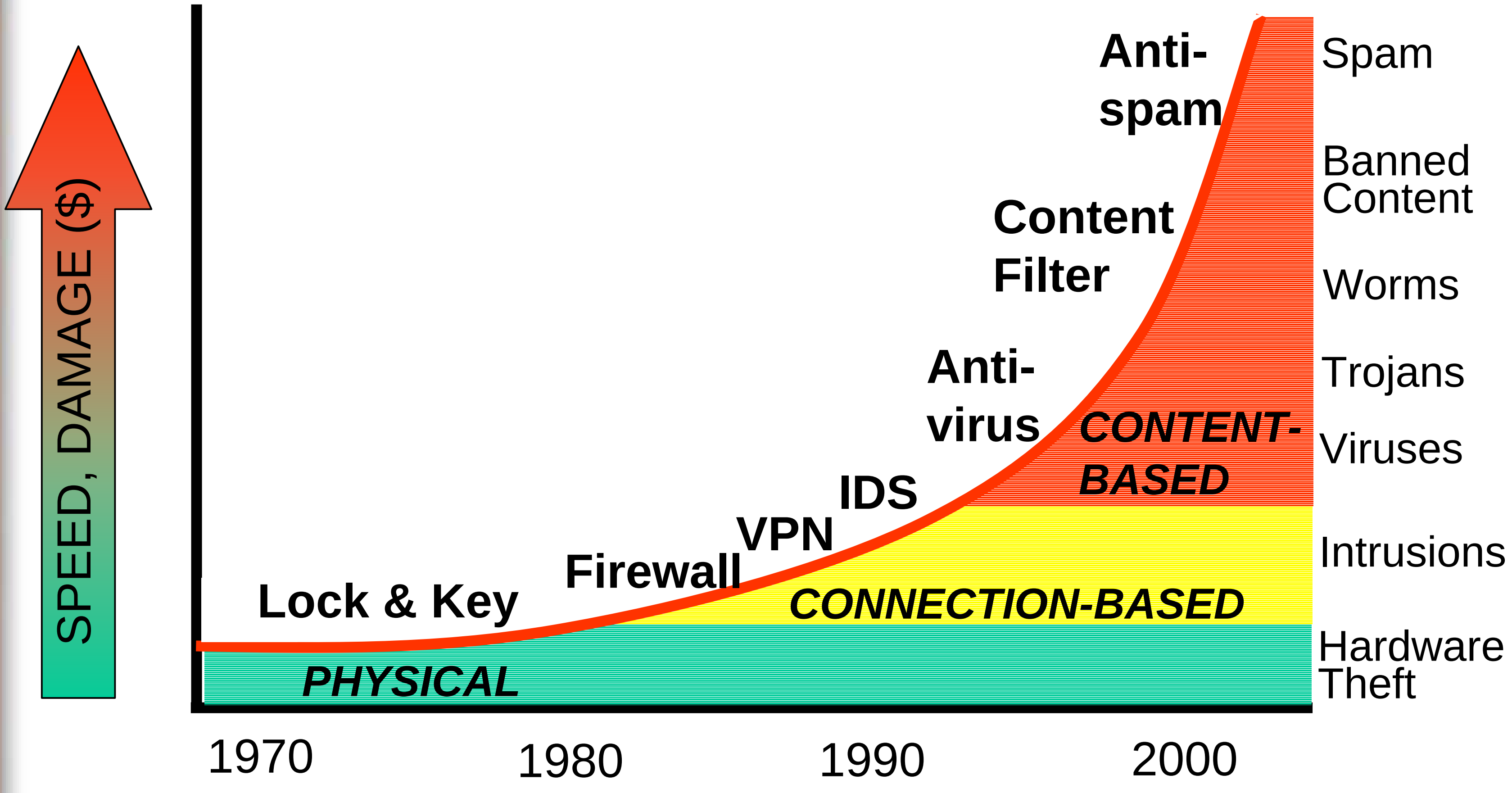
FORTINET

THE POWER IN NETWORK PROTECTION

資訊網路潛在威脅之探討分析

The Nature of Threats Has Evolved…

Major Pain Points for Organizations of all Types

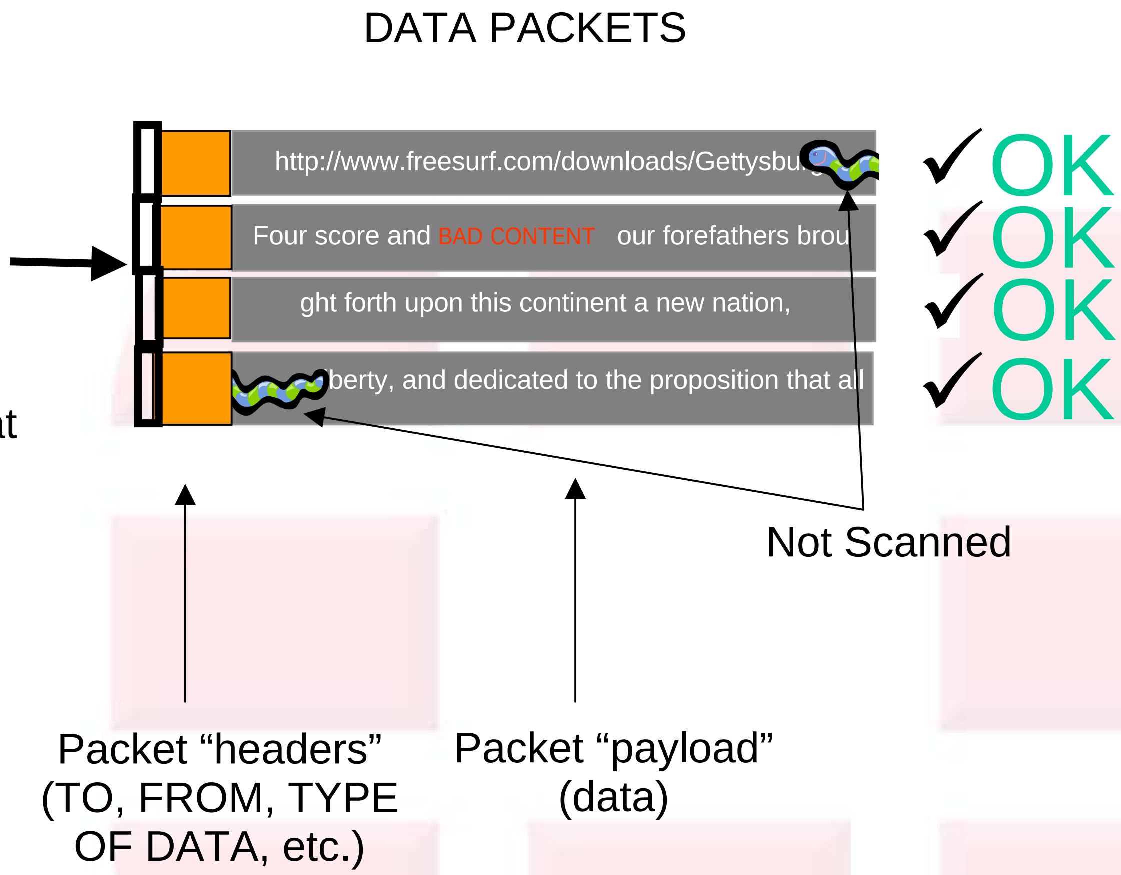


FORTINET

Firewalls Don’t Analyze Contents so they Miss Content Attacks

STATEFUL INSPECTION FIREWALL

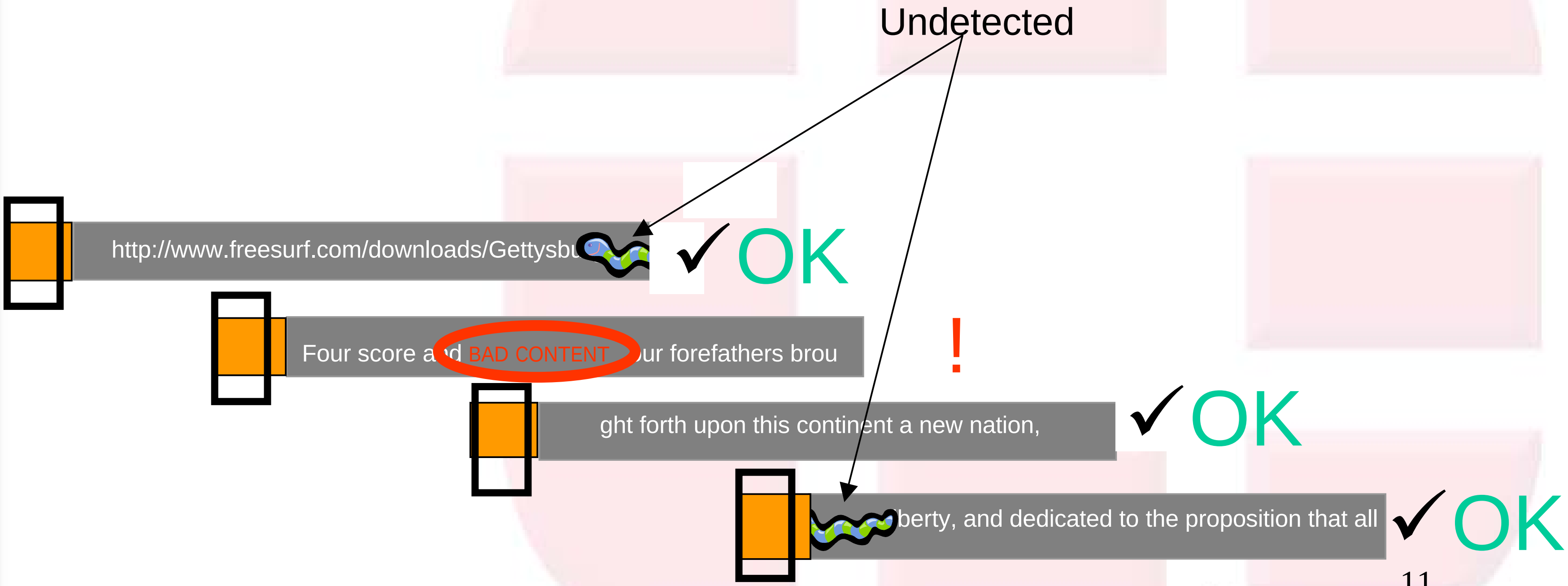
Inspects packet headers only – i.e. looks at the envelope, but not at what’s contained inside


DATA PACKETS
http://www.freesurf.com/downloads/Gettysbu
Four score and BAD CONTENT our forefathers brou
ght forth upon this continent a new nation,
berty, and dedicated to the proposition that all
✓OK
✓OK
✓OK
✓OK
Not Scanned
Packet “headers” (TO, FROM, TYPE OF DATA, etc.)
Packet “payload” (data)

Some Firewalls Claim to do “Deep Packet Inspection” – But They Still Miss a Lot

DEEP PACKET INSPECTION

Performs a packet-by-packet inspection of contents – but can easily miss complex attacks that span multiple packets

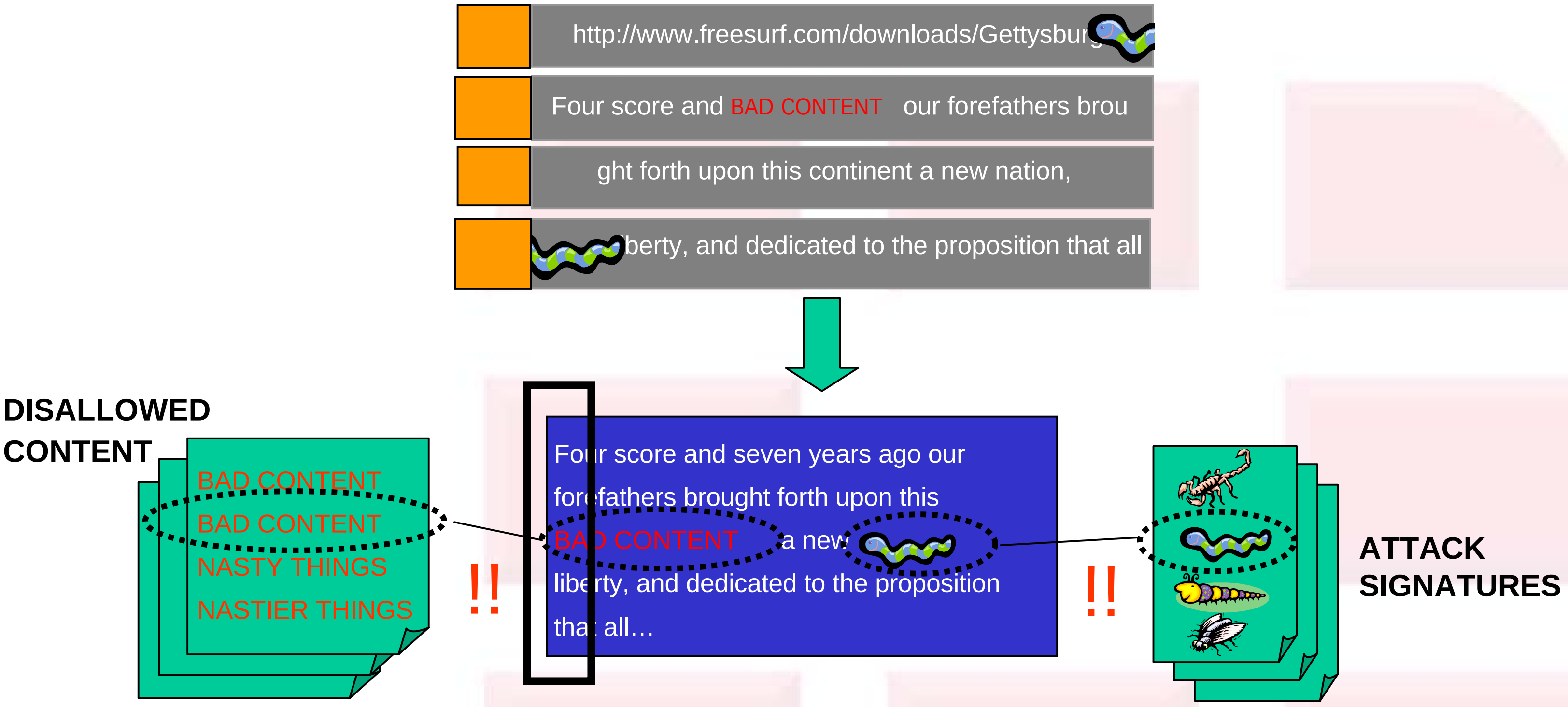


Undetected
http://www.freesurf.com/downloads/Gettysbu
✓OK
Four score and BAD CONTENT our forefathers brou
!
ght forth upon this continent a new nation,
✓OK
berty, and dedicated to the proposition that all
✓OK

To Stop Content-Based Threats Requires More than Deep Packet Inspection

COMPLETE CONTENT PROTECTION

1. Reassemble packets into content



http://www.freesurf.com/downloads/Gettysburg

Four score and BAD CONTENT our forefathers brou

ght forth upon this continent a new nation,

berty, and dedicated to the proposition that all

DISALLOWED CONTENT

BAD CONTENT

BAD CONTENT

NASTY THINGS

NASTIER THINGS

!!

Four score and seven years ago our forefathers brought forth upon this BAD CONTENT a new liberty, and dedicated to the proposition that all…

!!

ATTACK SIGNATURES

2. Compare against disallowed content and attack lists

使用網路銀行防毒、防駭缺一不可

Firewall

CA憑證/SSL

One Time Pass

記者歐陽宜珊／台北報導
2004-4-01 18:40

針對目前台灣出現網路銀行帳號被木馬程式竊取密碼而盜領的犯罪案例，雖然銀行立即向警方報案，且清查之後發現只有少數幾位受害者。若消費者的電腦被植入後門或是因為中毒，必須自行負擔損失。另外，若是習慣使用簡單密碼的用戶也要注意，駭客隨時可猜中密碼，而盜領銀行的錢。因此加強電腦防毒、防駭及強化身份認證機制成了當前重要的一環。

此次出現的案例，駭客是透過電子郵件或惡意網站等手法將木馬或後門程式植入受害者電腦，當使用者登入網路銀行時，木馬程式就將受害者在鍵盤上輸入的帳號及密碼等資料予以記錄，接著再將竊取到的資料，透過電子郵件或檔案傳送等手法傳至指定的網址，歹徒再透過「非約定帳戶」轉帳功能，盜領成功。

如果加裝用戶端數位憑證，也不能杜絕所有木馬或後門問題。只能增加入侵的複雜度，駭客還是有可能透過木馬竊走使用者密碼、數位憑證與私密金鑰。若使用IC卡或「一次密碼器」(Token)，也無法完全避免駭客利用木馬或後門進行盜領。駭客還是有可能在背景發出假交易或竄改交易內容，甚至可讓IC卡對假冒的交易內容進行數位簽章，除了利用此方式取得帳號外，多數人常用懶人密碼設定，雖然連續三次不對，帳號會被鎖定，不過若使用破解密碼的軟體，一次即可猜中。因此，如果要避免被駭客盜取密碼帳號，消費者在設定時，必須英文、數字混合使用，且至少應包含2個大小寫英文字母或符號、密碼與代號間不可相同。

網銀用戶須防堵木馬程式開後門竊密碼盜存款

Anti-Virus

IDS/IPS

(中央社記者韋樞台北四日電)

日前傳出數家網路銀行的客戶遭駭客盜領，事實上，此事件責任釐清後網路銀行並沒有安全疏失，主要原因是個人的安全防護出現大缺口，資訊安全廠商已經掌握到肇禍的木馬程式是Backdoor.Powerspider.B，駭客利用鍵盤側錄功能盜取存戶的密碼，將存戶的存款提領一空。

Backdoor.Powerspider.B，這類程式會偽裝成IE的名稱 iexpore.exe，駭客透過電子郵件或網頁，甚至是p2p程式等多種方式將此程式植入受害者電腦，利用鍵盤側錄的功能(keylogger)竊取機密資訊，再透過電子郵件的方式傳回駭客的電腦裡，駭客登入網路銀行後，透過「非約定轉帳」方式盜領存款。

至於駭客是如何植入後門及木馬程式，林育民分析，駭客利用病毒（Beagle、MyDoom、 Bugbear、系統漏洞、電子郵件，或透過色情、軟體破解或其他惡意網站，偽裝成可吸引使用者執行或下載的應用程式，或利用社交工程如MSN、Yahoo、Messenger、ICQ等途徑，植入或散布木馬程式。

網路銀行用戶要防杜被盜領，必須確認個人電腦的網路安全防護，除可偵測掃除木馬程式、鍵盤側錄程式的防毒功能外，進階型的個人防火牆，入侵偵測機制則是整合防護的標準配備，缺一不可。

對習慣性使用網路銀行的消費者而言，務必要養成良好的使用習慣，不任意開啟不明的電子郵件或附件，不隨意安裝或執行來路不明的軟體，不任意瀏覽色情或可能有惡意的網站，並關閉移除不必要的服務與程式，唯有確實在電腦安全防護和個人使用習慣上強化安全性，才能一面享受網路銀行的便利，一面照顧好自己的財物安全。930404

FORTINET™

THE POWER IN NETWORK PROTECTION

IPS can Protect everything --- Post-Sasser .

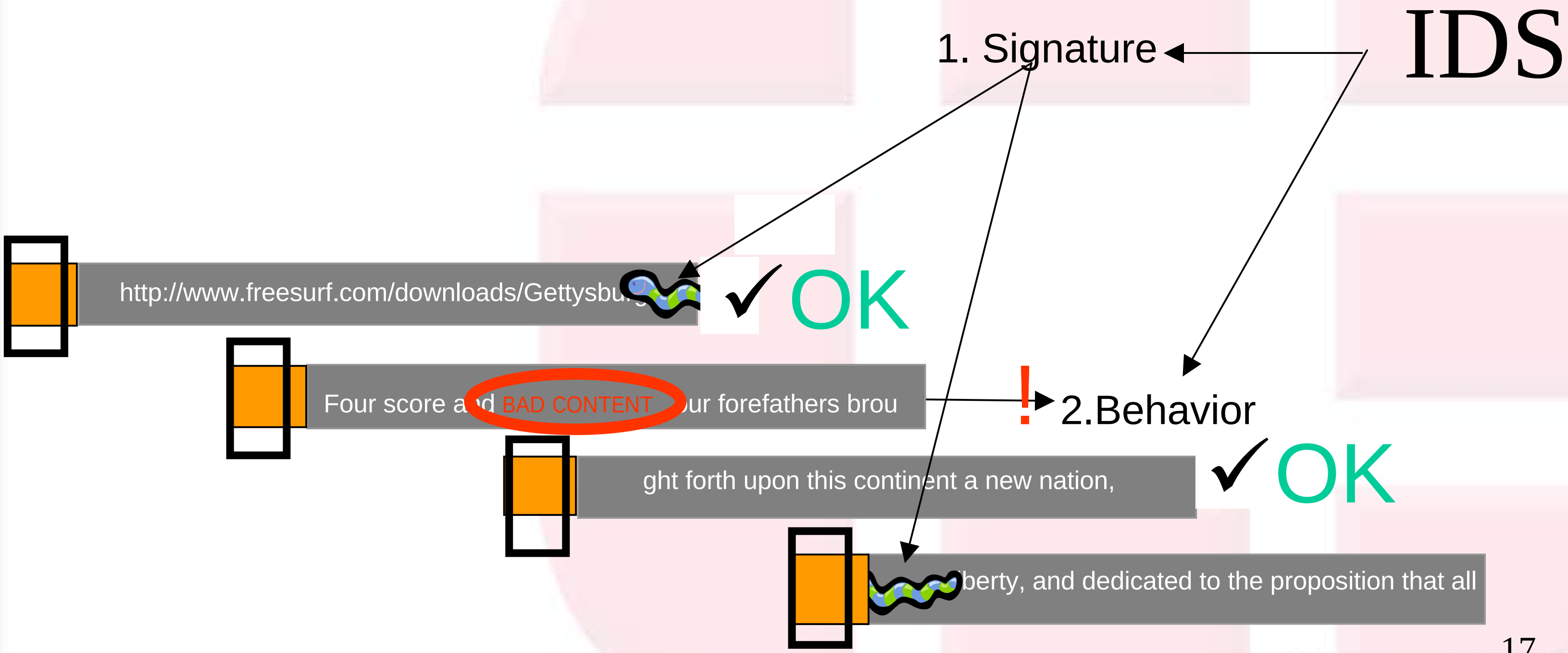
IPS Vendors Speak up ---- Post-Sasser

- Block worm & exploit viruses is trend
  - Antivirus is not important
  - Even NetSky can be blocked by IPS
- IPS is enough
  - Can block exploit worm, Trojans and Backdoor
- IF true, why T [illegible] Symantec … focus on pro [illegible] ? http,FTP,Em [illegible]

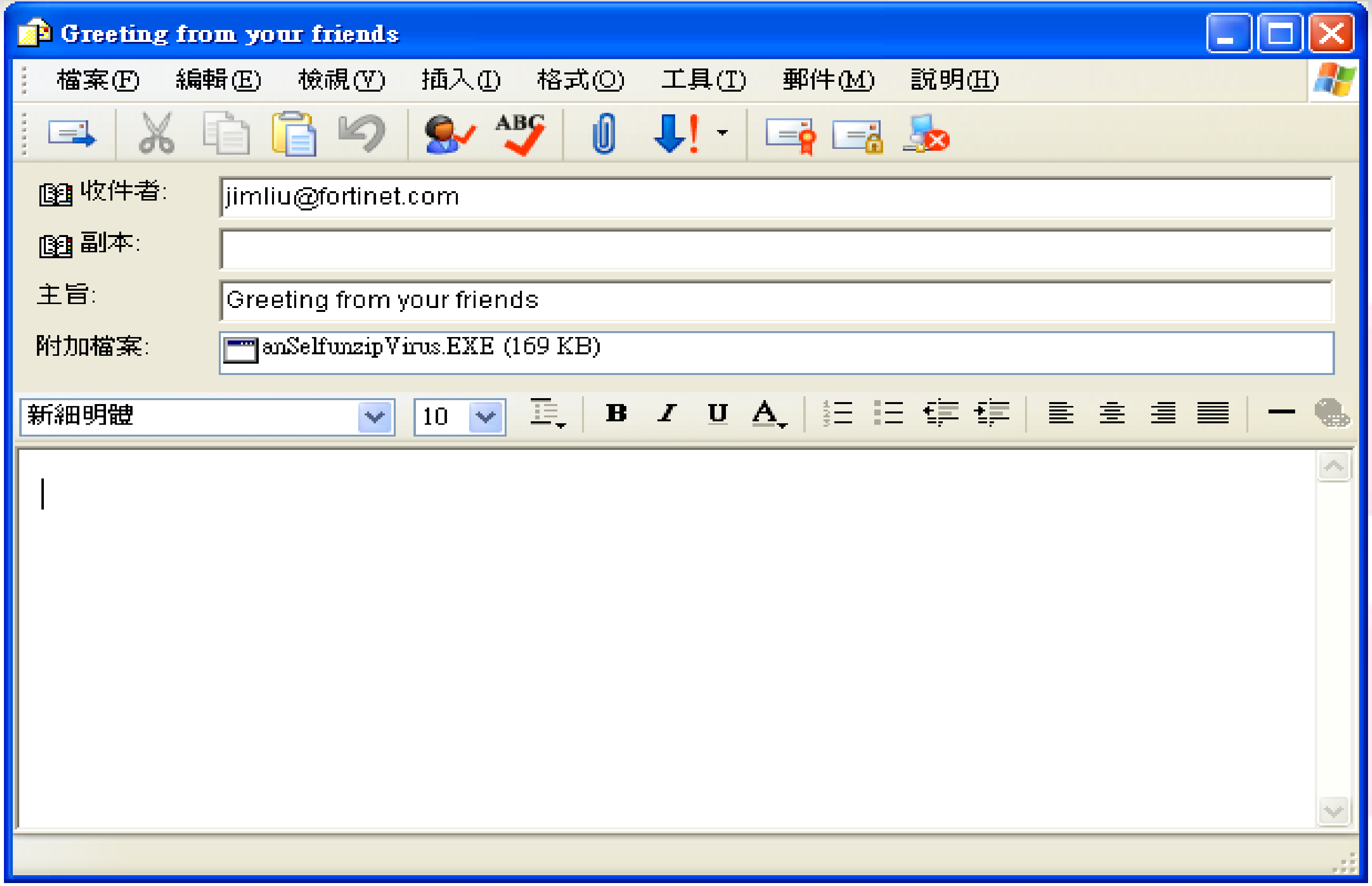
What is IDS ?

What does IDS work ?

Performs specific packets inspection and behavior analysis


1. Signature
IDS
http://www.freesurf.com/downloads/Gettysburg
✓OK
Four score and BAD CONTENT our forefathers brou
!
2.Behavior
ght forth upon this continent a new nation,
✓OK
berty, and dedicated to the proposition that all

The Fact is ……… (1/ 2)


Greeting from your friends
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 郵件(M) 說明(H)
新細明體
10
B I U A

收件者: jimliu@fortinet.com

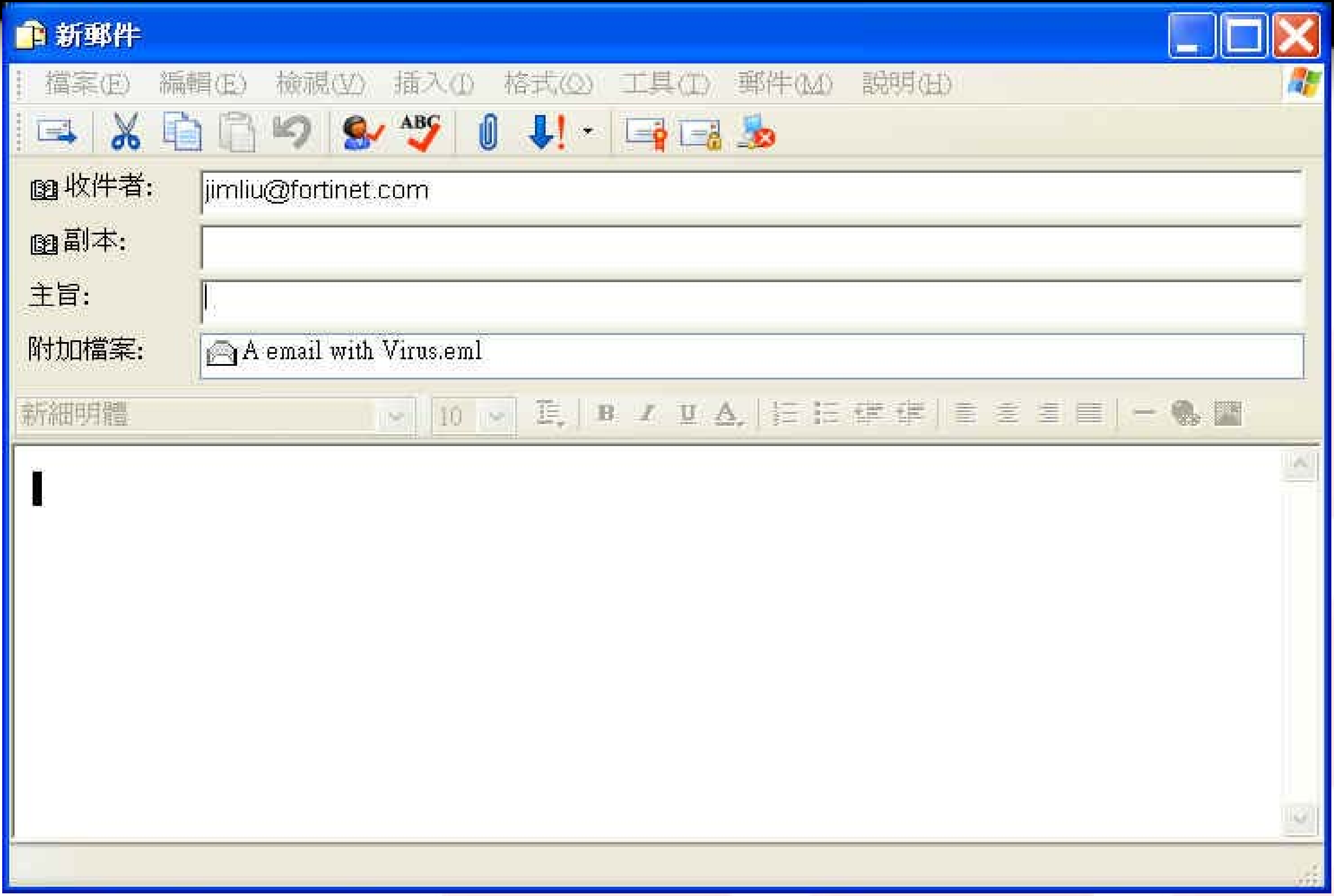
副本:

主旨: Greeting from your friends

附加檔案: anSelfunzipVirus.EXE (169 KB)

Only one level compression

The Fact is ……… (2/ 2)



新郵件

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 郵件(M) 說明(H)
新細明體
10

收件者: jimliu@fortinet.com

副本:

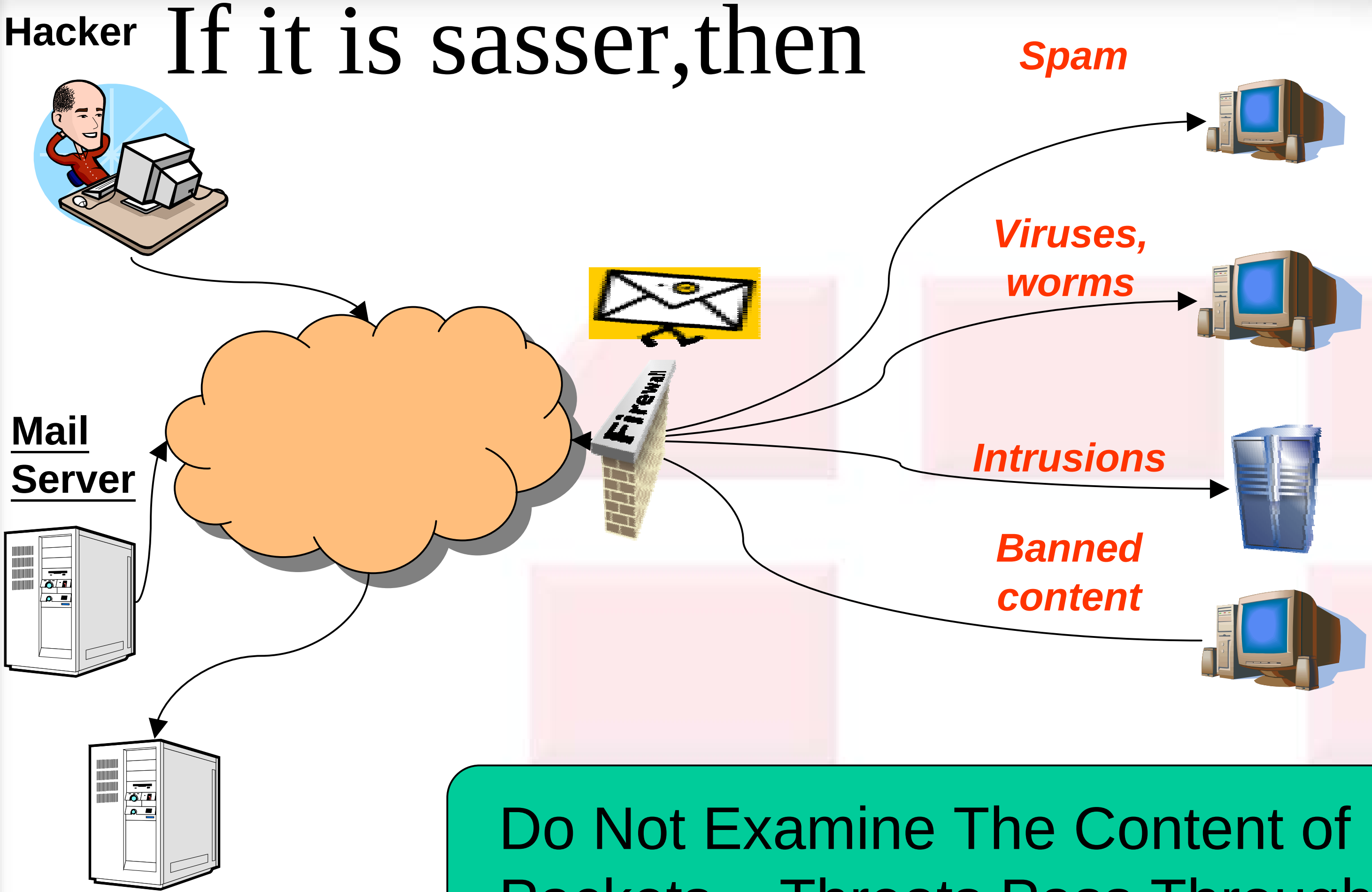
主旨:

附加檔案: A email with Virus.eml

Or attached a email with Viruses

Conventional/Single Point Security Solution Do Not Solve these Problems

If it is sasser,then



www.find_a new job.com
www.free music.com
www.pornography.com

Do Not Examine The Content of Data Packets – Threats Pass Through

Protocol-based Antivirus Benefits

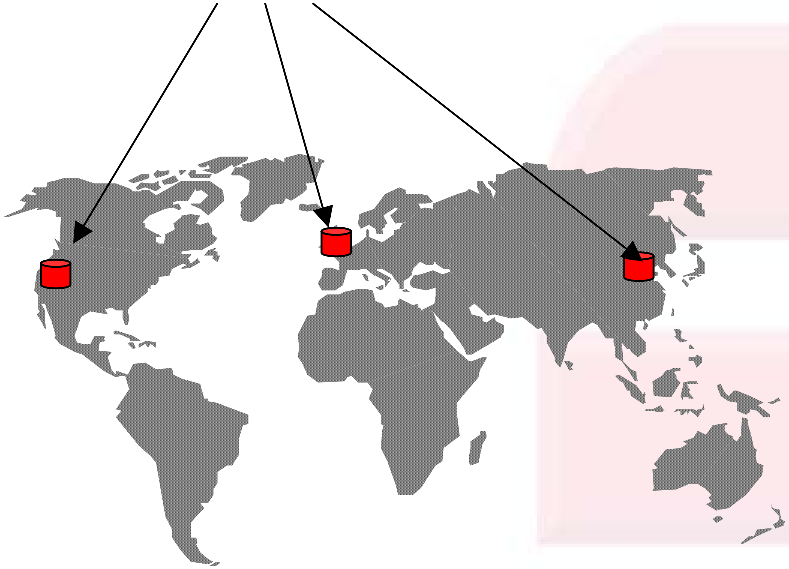
- According to protocol
  - to adapt different kinds of file format or Characteristic of different application.

    i.e. like compression file type , ZIP, RAR….

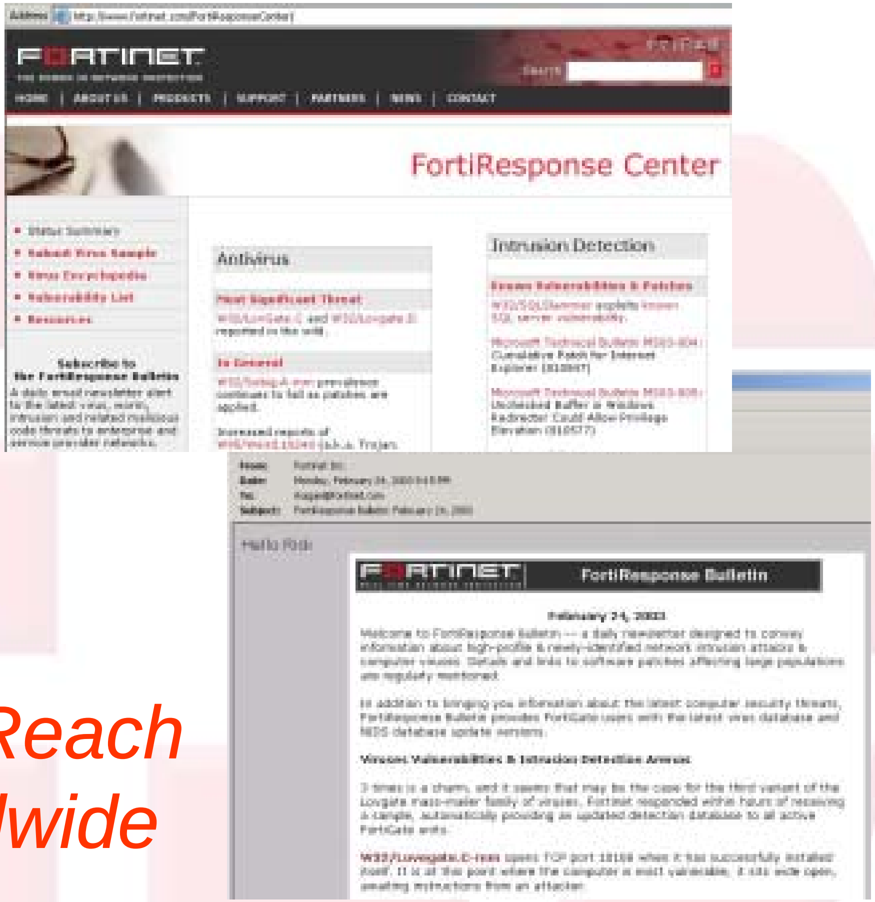
    outlook, outlook express or Unix Mailbox

World-Wide based Real time Update Center
Ensure Rapid Response to New Threats

Fortinet Threat Response Team and Update Distribution Servers



FortiProtection Center
Web Portal & email Bulletins



Address http://www.fortinet.com/FortiResponseCenter/

HOME | ABOUT US | PRODUCTS | SUPPORT | PARTNERS | NEWS | CONTACT

FortiResponse Center

- Status Summary
- Submit Virus Sample
- Virus Encyclopedia
- Vulnerability List
- Resources

Subscribe to
the FortiResponse Bulletin
A daily email newsletter alert to the latest virus, worm, intrusion and related malicious code threats to enterprise and service provider networks.

Antivirus

Most Significant Threat
W32/Lovgate.C and W32/Lovgate.B reported in the wild.

In General
W32/Sobig.A-mm prevalence continues to fall as patches are applied.

Increased reports of W95/Weird.10240 (a.k.a. Trojan

Intrusion Detection

Known Vulnerabilities & Patches
W32/SQLSlammer exploits known SQL server vulnerability.

Microsoft Technical Bulletin MS03-004: Cumulative Patch for Internet Explorer (810847)

Microsoft Technical Bulletin MS03-005: Unchecked Buffer in Windows Redirector Could Allow Privilege Elevation (810577)

From: Fortinet Inc
Date: Monday, February 24, 2003 [illegible]
To: [illegible]@fortinet.com
Subject: FortiResponse Bulletin February 24, 2003

Hello Rob:

FortiResponse Bulletin

February 24, 2003

Welcome to FortiResponse Bulletin — a daily newsletter designed to convey information about high-profile & newly-identified network intrusion attacks & computer viruses. Details and links to software patches affecting large populations are regularly mentioned.

In addition to bringing you information about the latest computer security threats, FortiResponse Bulletin provides FortiGate users with the latest virus database and NIDS database update versions.

Viruses, Vulnerabilities & Intrusion Detection Arrivals

3 times is a charm, and it seems that may be the case for the third variant of the Lovgate mass-mailer family of viruses. Fortinet responded within hours of receiving a sample, automatically providing an updated detection database to all active FortiGate units.

W32/Lovgate.C-mm opens TCP port 10168 when it has successfully installed itself. It is at this point where the computer is most vulnerable; it sits wide open, awaiting instructions from an attacker.

Automatic Updates Can Reach All FortiGate Units Worldwide in Under 5 Minutes

Dynamic Real time Attack Response Combines the Best of AV, NIDS and IDP

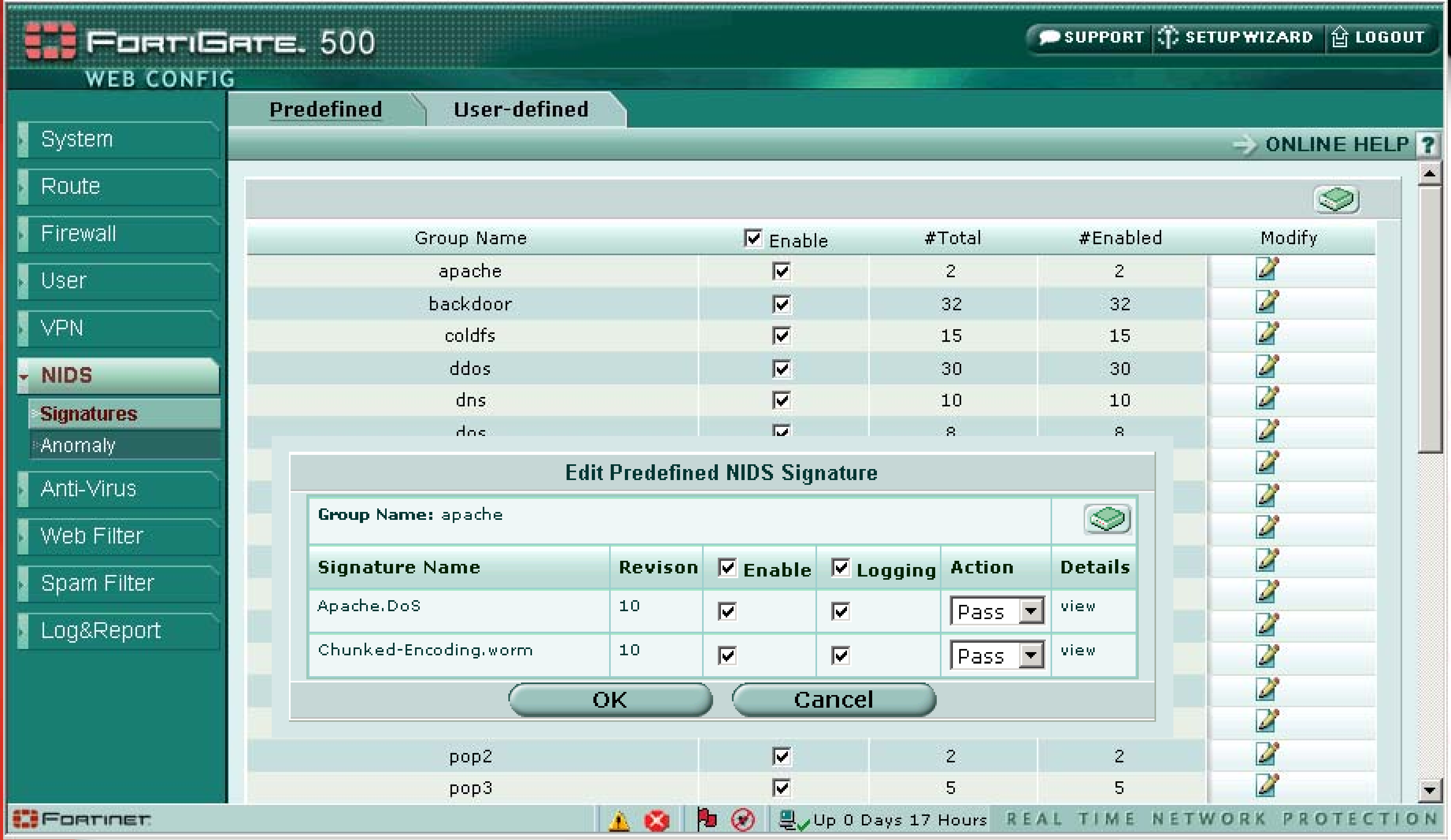
- Multiple detection mechanisms
  - AV signatures (application layer, content scan)
  - Intrusion signatures (protocol layer, content & behavior)

- Reduction in false positives and the amount of data analysis
  - Policy-based IPS applies scanning only where needed

- Multiple prevention mechanisms
  - Packet drop
  - Port closure
  - TCP reset
  - Traffic limit (e.g. P2P apps)
  - File delete/quarantine

All dynamically updatable via the FortiProtection Network

NIPS Signatures



Group Name	☑ Enable	#Total	#Enabled	Modify
apache	☑	2	2	✎
backdoor	☑	32	32	✎
coldfs	☑	15	15	✎
ddos	☑	30	30	✎
dns	☑	10	10	✎
dos	☑	8	8	✎
pop2	☑	2	2	✎
pop3	☑	5	5	✎

Edit Predefined NIDS Signature

Group Name: apache

Signature Name	Revison	☑ Enable	☑ Logging	Action	Details
Apache.DoS	10	☑	☑	Pass	view
Chunked-Encoding.worm	10	☑	☑	Pass	view

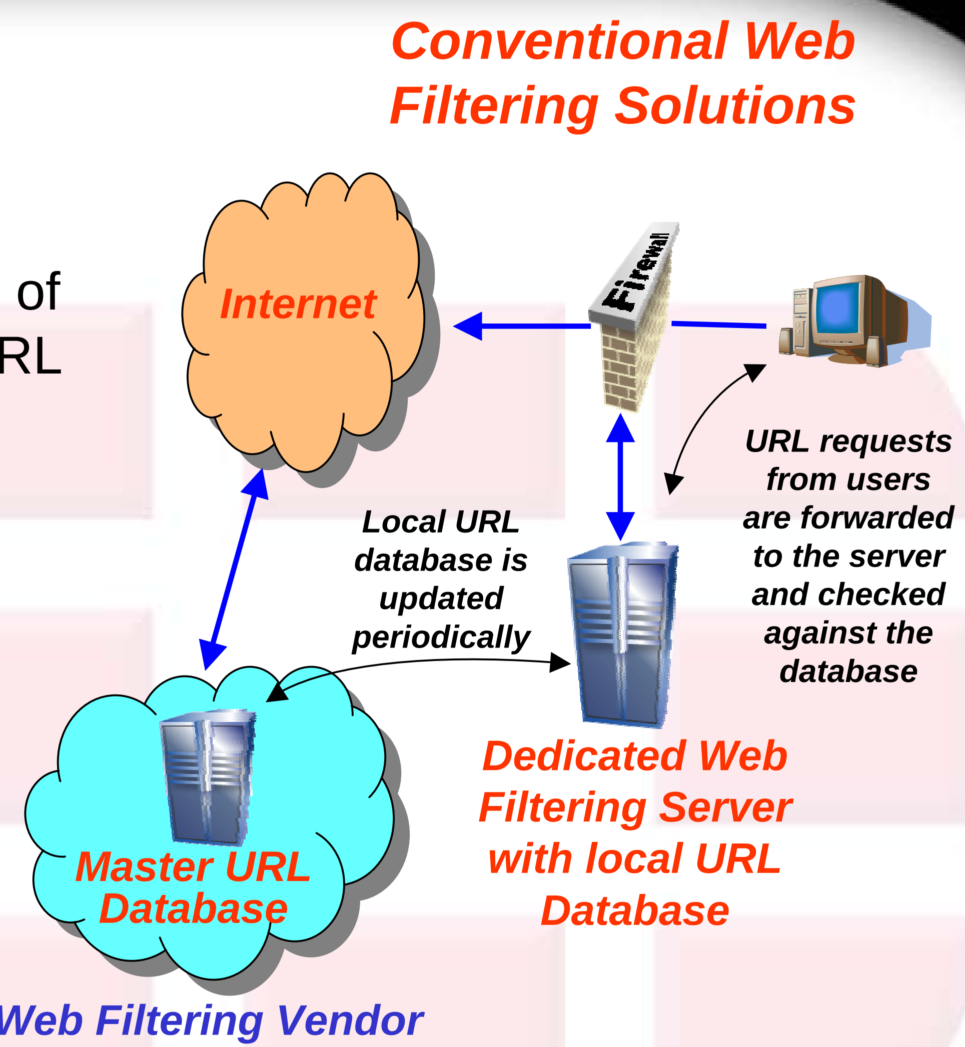
FORTINET™

THE POWER IN NETWORK PROTECTION

A New Approach for Content filtering

Limitations of Conventional Software-Based Web Filtering Solutions

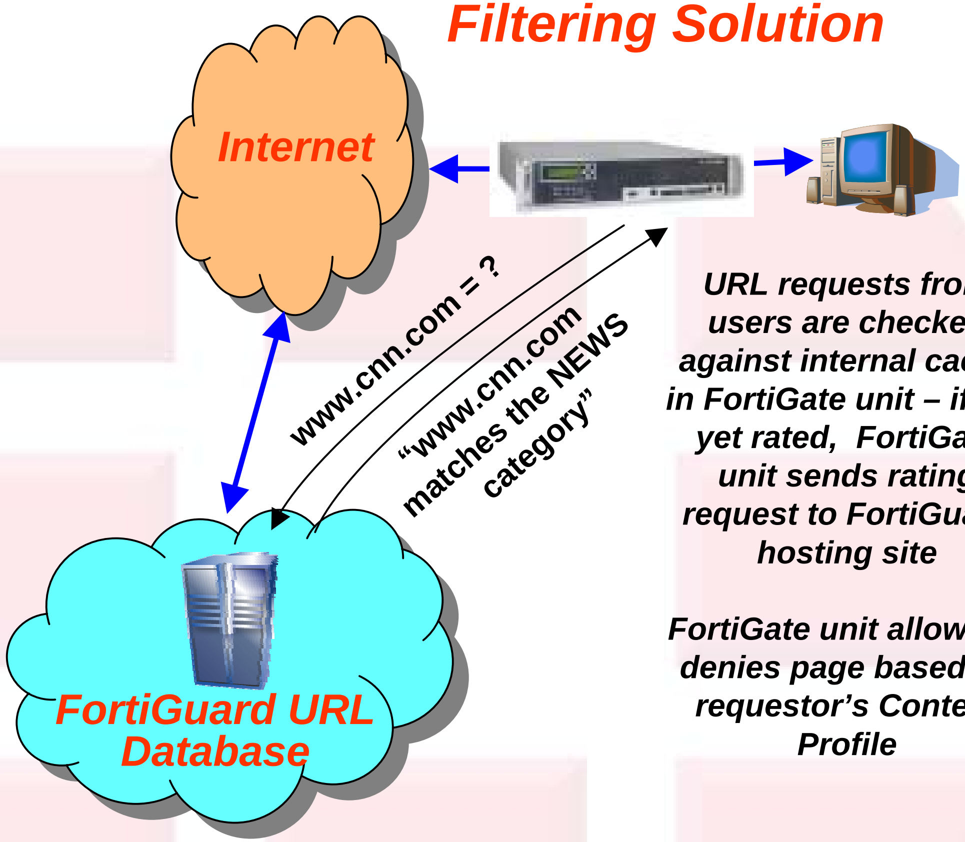
- Requires a dedicated server
- Requires periodic update of large (multi-megabyte) URL database
- Missed and incorrect ratings between updates
- High cost


Conventional Web Filtering Solutions
Internet
Firewall
Local URL database is updated periodically
URL requests from users are forwarded to the server and checked against the database
Master URL Database
Dedicated Web Filtering Server with local URL Database
Web Filtering Vendor

The Fortinet Solution: FortiGate Antivirus Firewalls + FortiGuard Service

- No additional hardware required
- No need to download large database to FortiGate units
- URL ratings are always up to date
- Local FortiGate caching of ratings greatly improves performance
- FortiGate solution also scans HTML content for keywords/phrases
- Lower cost
- Multi-language recognition
- **Reduction in false positives**
  - **Policy-based IPS applies scanning only where needed**

FortiGuard Web Filtering Solution

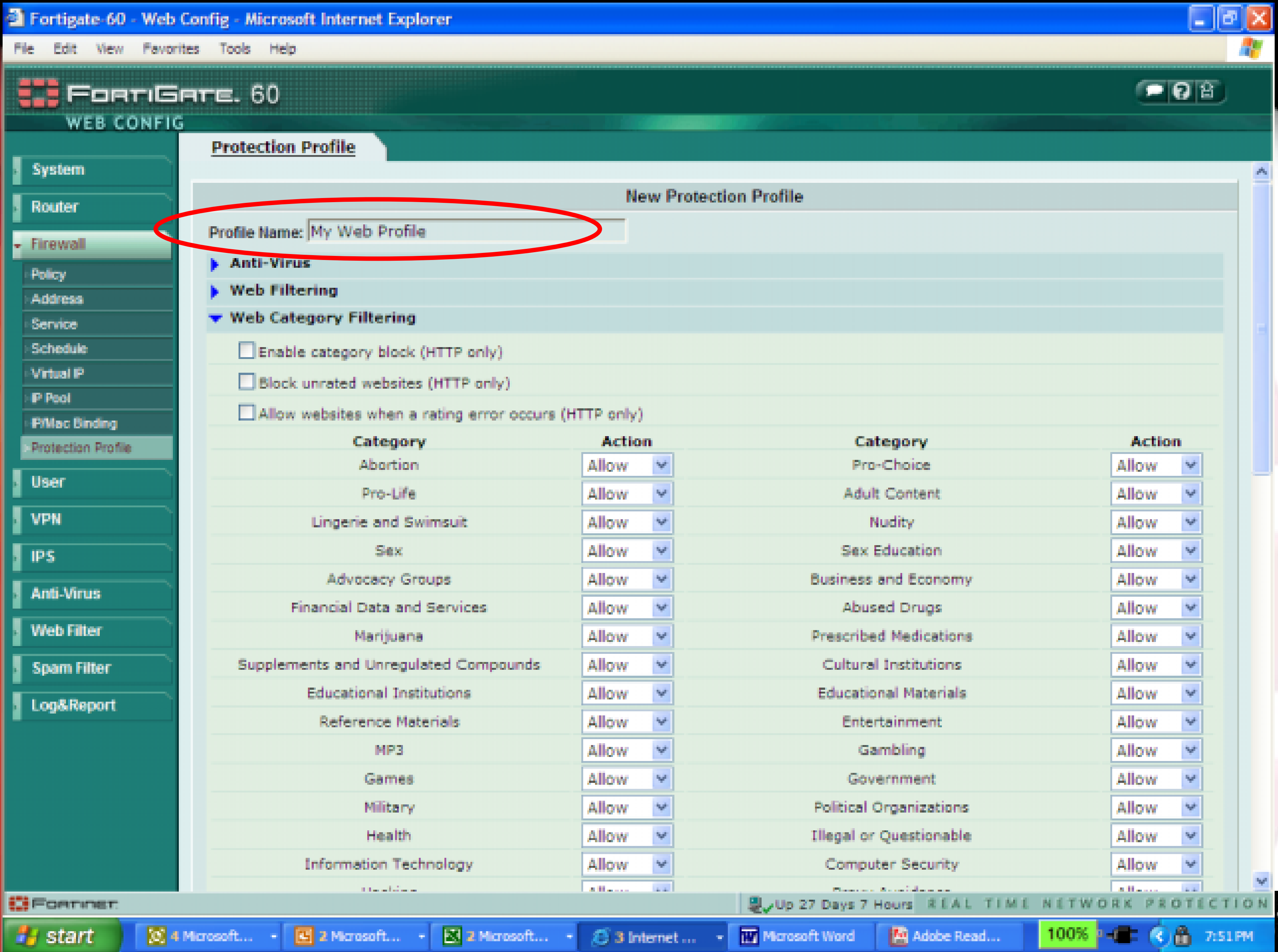


URL requests from users are checked against internal cache in FortiGate unit – if not yet rated, FortiGate unit sends rating request to FortiGuard hosting site

FortiGate unit allows or denies page based on requestor's Content Profile

FortiGuard Hosting Sites (data mining) (Worldwide)

Web Profiles Support 80 Content Categories



New Protection Profile

Profile Name: My Web Profile

- Anti-Virus
- Web Filtering
- Web Category Filtering

□ Enable category block (HTTP only)

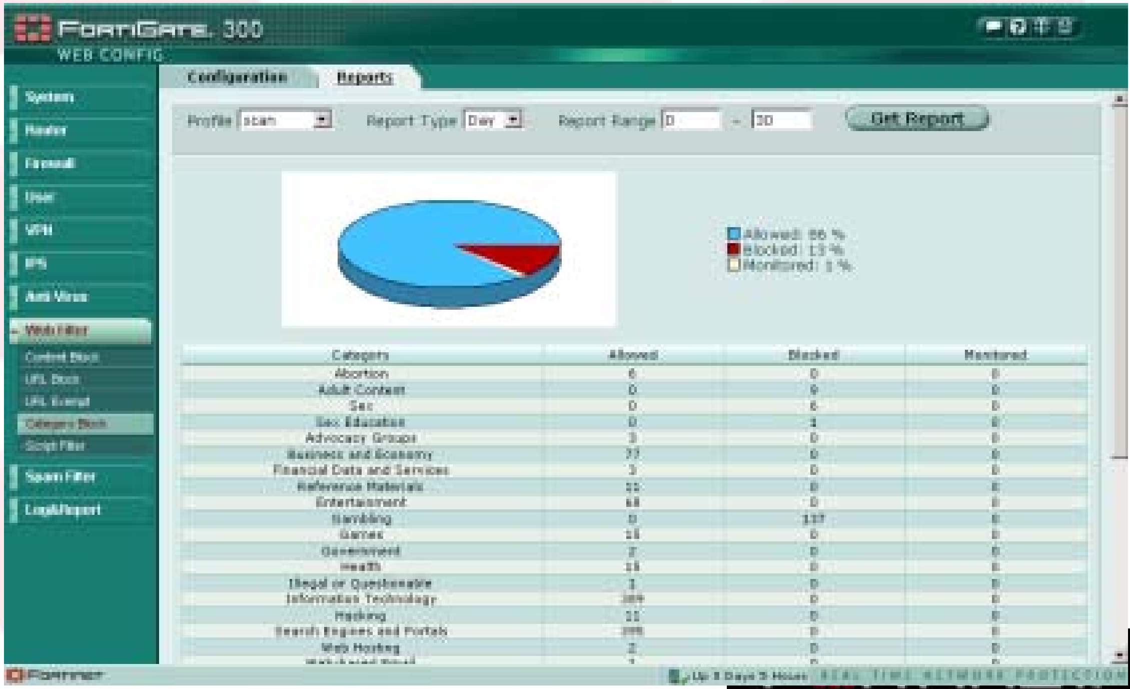
□ Block unrated websites (HTTP only)

□ Allow websites when a rating error occurs (HTTP only)

Category	Action	Category	Action
Abortion	Allow	Pro-Choice	Allow
Pro-Life	Allow	Adult Content	Allow
Lingerie and Swimsuit	Allow	Nudity	Allow
Sex	Allow	Sex Education	Allow
Advocacy Groups	Allow	Business and Economy	Allow
Financial Data and Services	Allow	Abused Drugs	Allow
Marijuana	Allow	Prescribed Medications	Allow
Supplements and Unregulated Compounds	Allow	Cultural Institutions	Allow
Educational Institutions	Allow	Educational Materials	Allow
Reference Materials	Allow	Entertainment	Allow
MP3	Allow	Gambling	Allow
Games	Allow	Government	Allow
Military	Allow	Political Organizations	Allow
Health	Allow	Illegal or Questionable	Allow
Information Technology	Allow	Computer Security	Allow
Hacking	Allow	Proxy Avoidance	Allow

A Range of Logging and Reporting Options

- Logging
  - FortiGate unit logs the source IP, destination IP, requested URL, action (allowed/denied), and content category
- Built-in reporting
  - Graph in the FortiGate GUI shows web usage by category
- Additional reporting
  - Logs are compatible with 3rd party reporting tools, such as eIQnetworks Firewall Analyzer / SecureExp



Profile scan Report Type Day Report Range 0 - 30

🟦 Allowed: 86 %
🟥 Blocked: 13 %
□ Monitored: 1 %

Category	Allowed	Blocked	Monitored
Abortion	6	0	0
Adult Content	0	9	0
Sex	0	6	0
Sex Education	0	1	0
Advocacy Groups	3	0	0
Business and Economy	77	0	0
Financial Data and Services	3	0	0
Reference Materials	11	0	0
Entertainment	68	0	0
Gambling	0	137	0
Games	15	0	0
Government	7	0	0
Health	18	0	0
Illegal or Questionable	1	0	0
Information Technology	189	0	0
Hacking	11	0	0
Search Engines and Portals	295	0	0
Web Hosting	2	0	0

FORTINET™

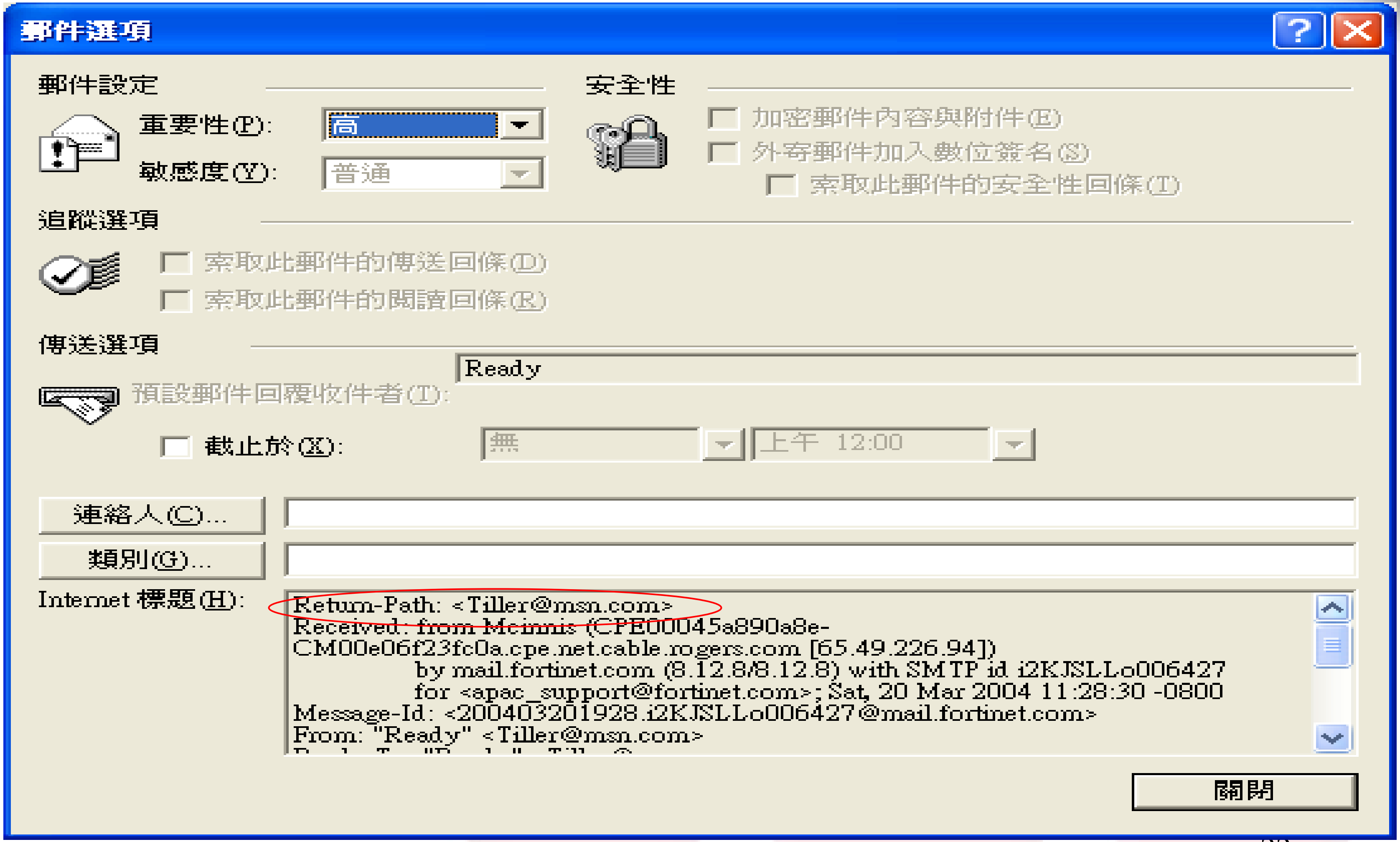
THE POWER IN NETWORK PROTECTION

A BASIC Anti-SPAM skill

Email Content Filtering (Antispam) Enhancements

- Check & Mark Messages with Signs of SPAM:
  - Keywords & phrases in message body and subject line
  - Blacklist of known bad spam senders
  - Invalid return email address (DNS check)
  - Spoofing (MIME header check)
- Block SMTP Messages based on:
  - IP address Black/White list
  - IP-based checks against the Real-time Blackhole list (RBL) and the Open Relay Database (ORDB)
  - Reverse DNS lookups

Anti-Spam



郵件選項

郵件設定

重要性(P): 高

敏感度(Y): 普通

安全性

□ 加密郵件內容與附件(E)

□ 外寄郵件加入數位簽名(S)

□ 索取此郵件的安全性回條(T)

追蹤選項

□ 索取此郵件的傳送回條(D)

□ 索取此郵件的閱讀回條(R)

傳送選項

預設郵件回覆收件者(T): Ready

□ 截止於(X): 無 上午 12:00

連絡人(C)...

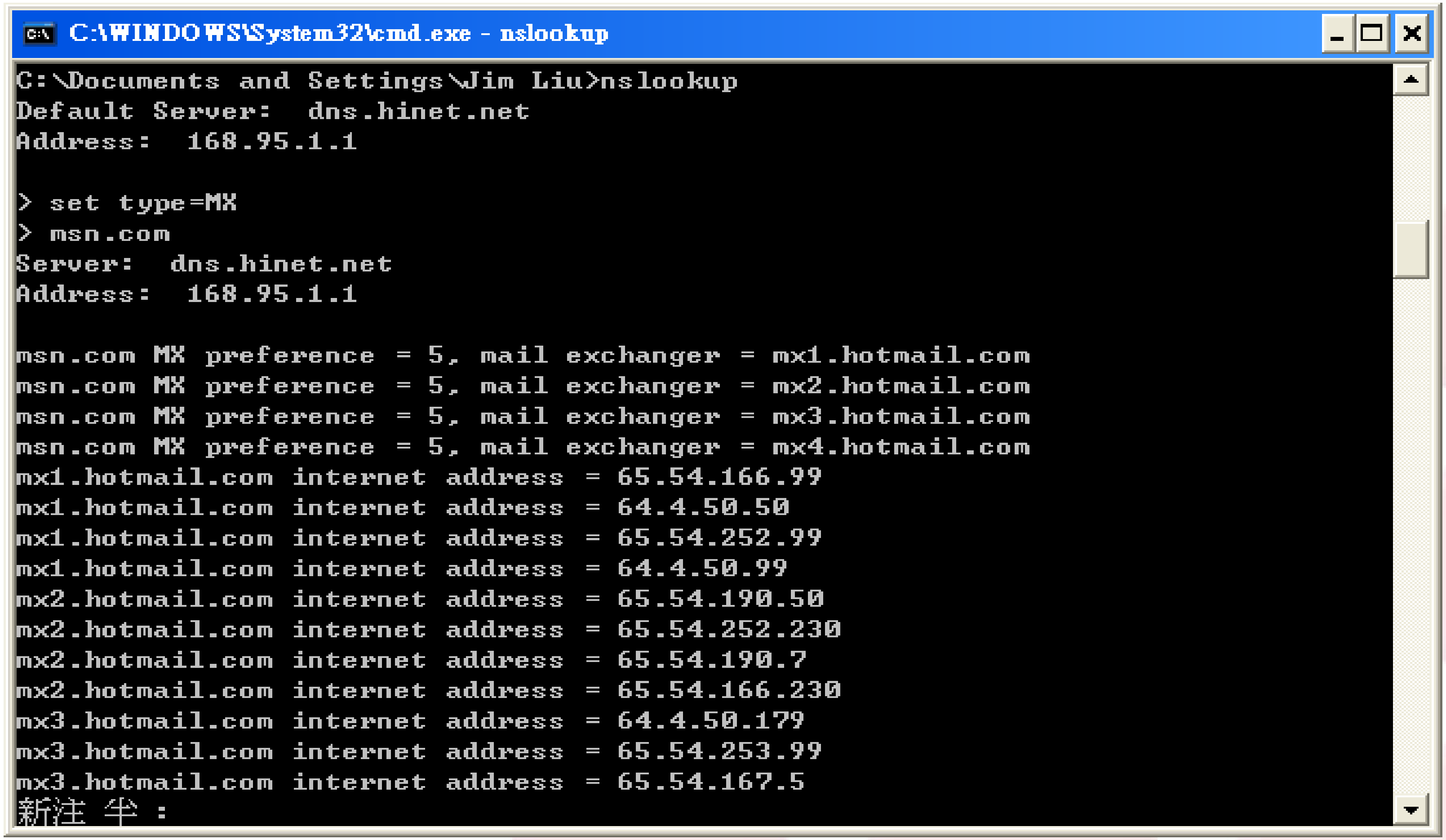
類別(G)...

Internet 標題(H):

```
Return-Path: <Tiller@msn.com>
Received: from Mcinnis (CPE00045a890a8e-
CM00e06f23fc0a.cpe.net.cable.rogers.com [65.49.226.94])
              by mail.fortinet.com (8.12.8/8.12.8) with SMTP id i2KJSLLo006427
              for <apac_support@fortinet.com>; Sat, 20 Mar 2004 11:28:30 -0800
Message-Id: <200403201928.i2KJSLLo006427@mail.fortinet.com>
From: "Ready" <Tiller@msn.com>
```

關閉

Anti-Spam

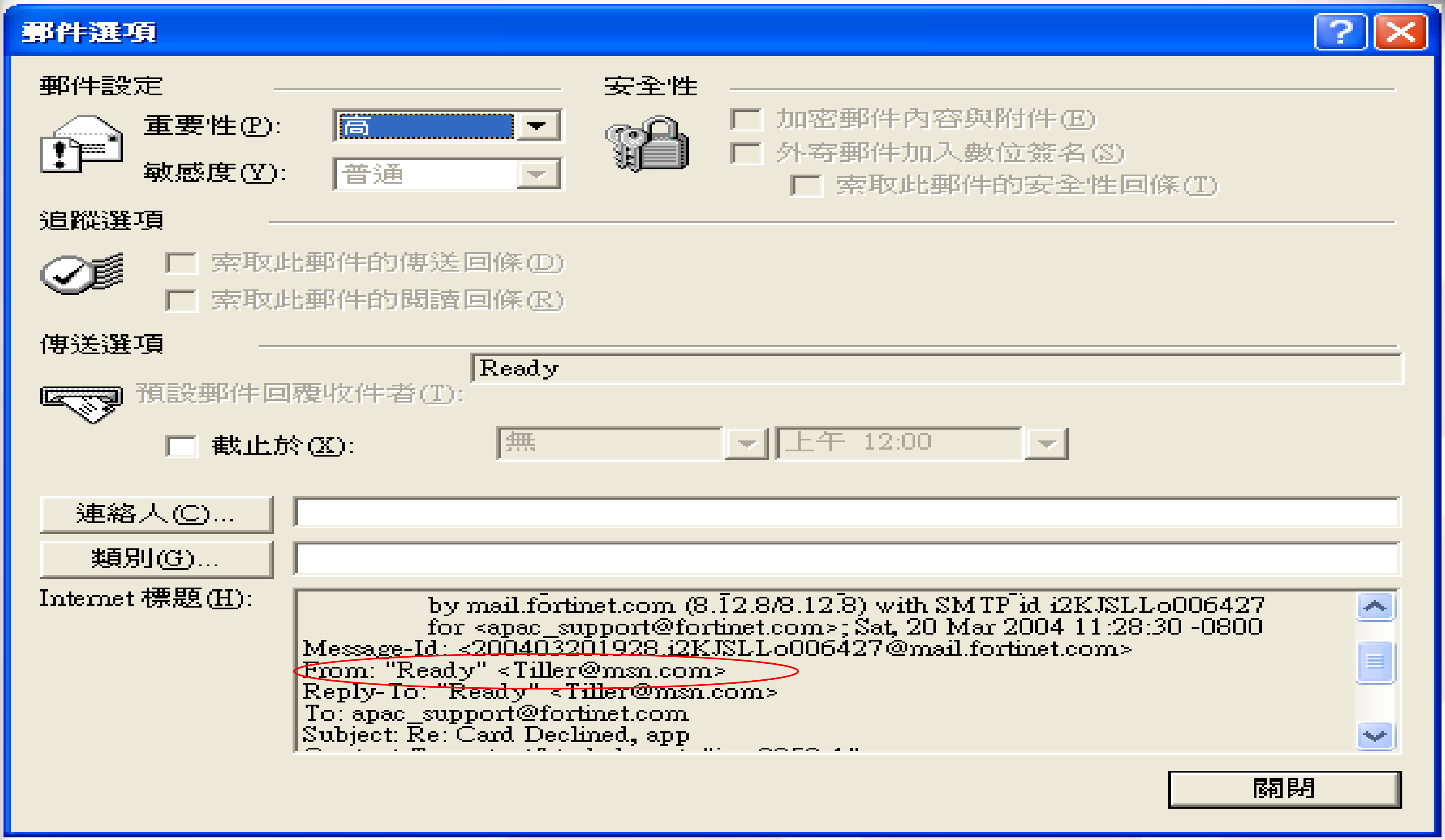


```
C:\Documents and Settings\Jim Liu>nslookup
Default Server:  dns.hinet.net
Address:  168.95.1.1

> set type=MX
> msn.com
Server:  dns.hinet.net
Address:  168.95.1.1

msn.com MX preference = 5, mail exchanger = mx1.hotmail.com
msn.com MX preference = 5, mail exchanger = mx2.hotmail.com
msn.com MX preference = 5, mail exchanger = mx3.hotmail.com
msn.com MX preference = 5, mail exchanger = mx4.hotmail.com
mx1.hotmail.com internet address = 65.54.166.99
mx1.hotmail.com internet address = 64.4.50.50
mx1.hotmail.com internet address = 65.54.252.99
mx1.hotmail.com internet address = 64.4.50.99
mx2.hotmail.com internet address = 65.54.190.50
mx2.hotmail.com internet address = 65.54.252.230
mx2.hotmail.com internet address = 65.54.190.7
mx2.hotmail.com internet address = 65.54.166.230
mx3.hotmail.com internet address = 64.4.50.179
mx3.hotmail.com internet address = 65.54.253.99
mx3.hotmail.com internet address = 65.54.167.5
新注 半 :
```

Anti-Spam



郵件選項

郵件設定

重要性(P): 高

敏感度(V): 普通

安全性

□ 加密郵件內容與附件(E)

□ 外寄郵件加入數位簽名(S)

□ 索取此郵件的安全性回條(T)

追蹤選項

□ 索取此郵件的傳送回條(D)

□ 索取此郵件的閱讀回條(R)

傳送選項

預設郵件回覆收件者(T): Ready

□ 截止於(X): 無 上午 12:00

連絡人(C)...

類別(G)...

Internet 標題(H):

```
          by mail.fortinet.com (8.12.8/8.12.8) with SMTP id i2KJSLLo006427
          for <apac_support@fortinet.com>; Sat, 20 Mar 2004 11:28:30 -0800
Message-Id: <200403201928.i2KJSLLo006427@mail.fortinet.com>
From: "Ready" <Tiller@msn.com>
Reply-To: "Ready" <Tiller@msn.com>
To: apac_support@fortinet.com
Subject: Re: Card Declined, app
```

關閉

RBL Server-List

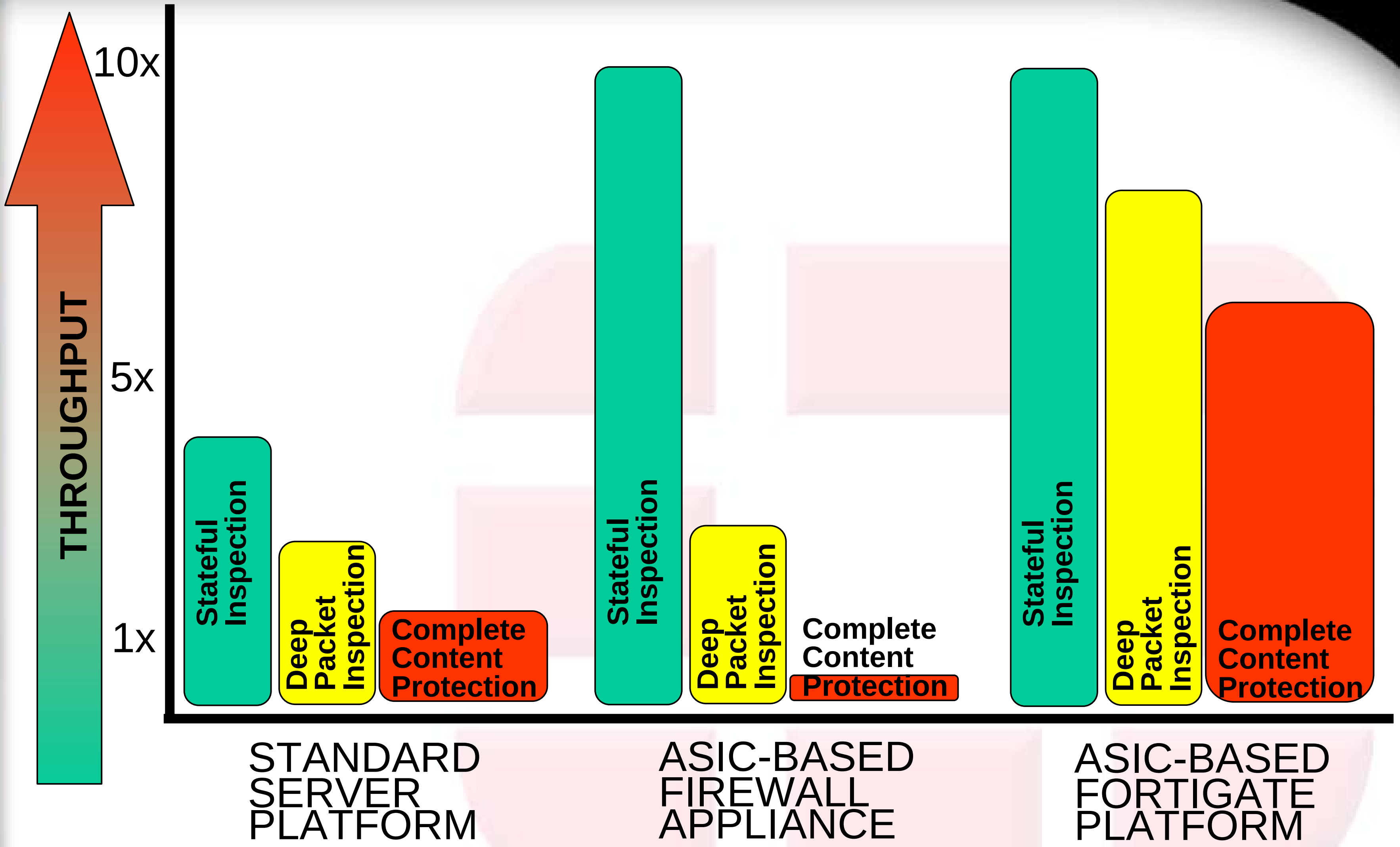
- rbl.maps.vix.com
- dul.maps.vix.com
- relays.orbs.org
- bl.spamcop.net
- cbl.abuseat.org
- dnsbl.njabl.org
- dnsbl.sorbs.net

FORTINET™

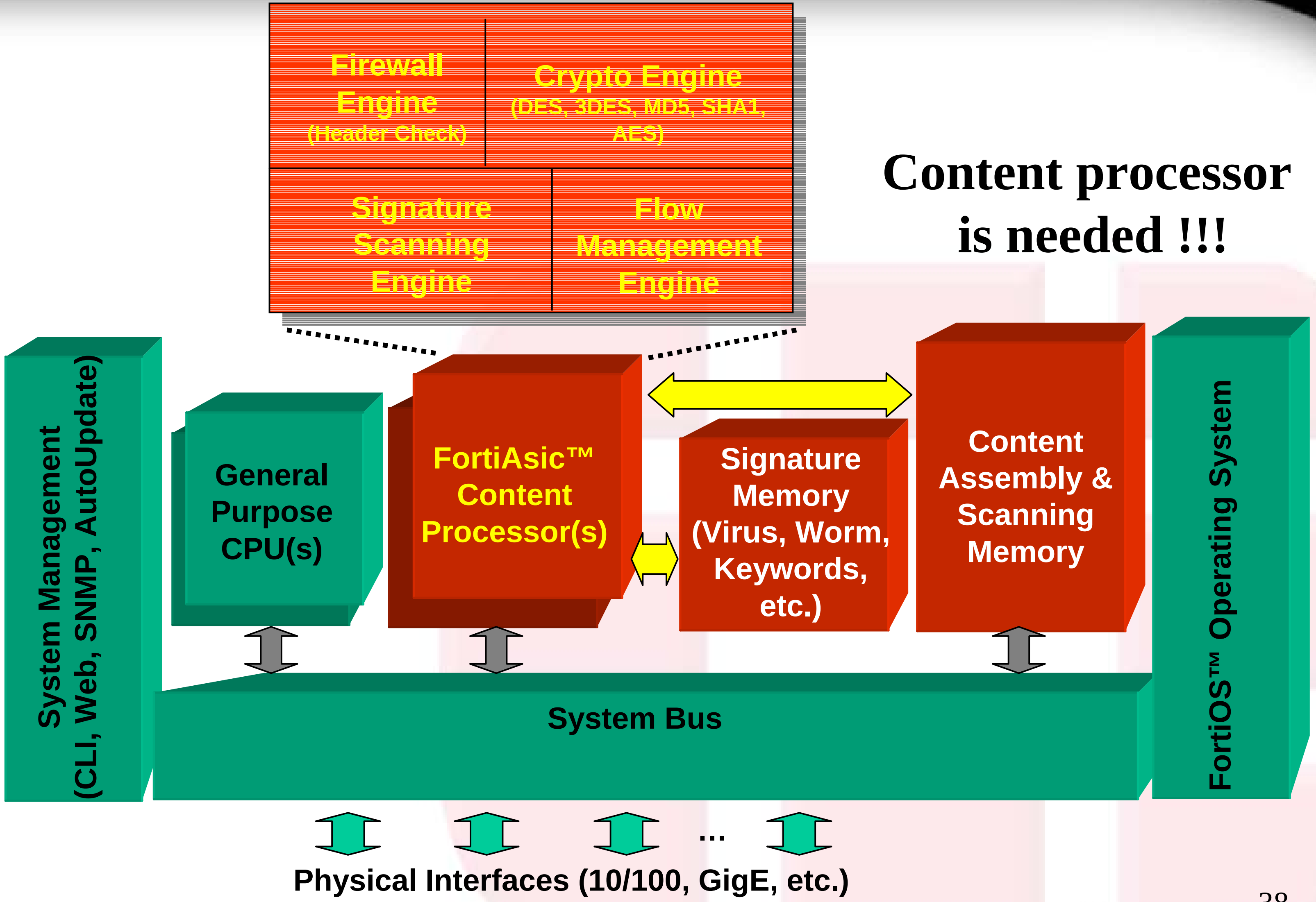
THE POWER IN NETWORK PROTECTION

Why everybody talk about ASIC?

The ASIC-Based FortiGate Platforms Provide Better Protection and Higher Performance



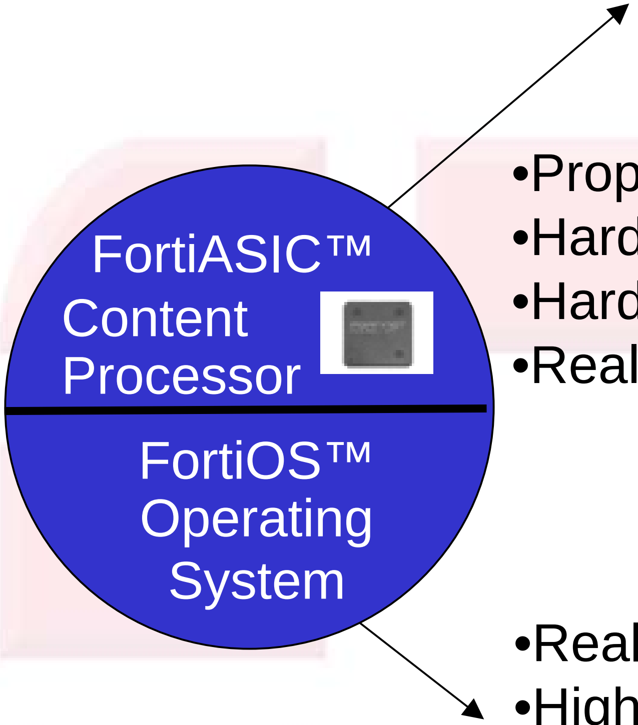
What’s real hardware-based Seurity Box ?


Firewall Engine (Header Check)
Crypto Engine (DES, 3DES, MD5, SHA1, AES)
Signature Scanning Engine
Flow Management Engine
System Management (CLI, Web, SNMP, AutoUpdate)
General Purpose CPU(s)
FortiAsic™ Content Processor(s)
Signature Memory (Virus, Worm, Keywords, etc.)
Content Assembly & Scanning Memory
FortiOS™ Operating System
System Bus
…
Physical Interfaces (10/100, GigE, etc.)

Content processor is needed !!!

Fortinet Developed a Unique Architecture for Complete, Real-Time Network Protection

CORE TECHNOLOGY

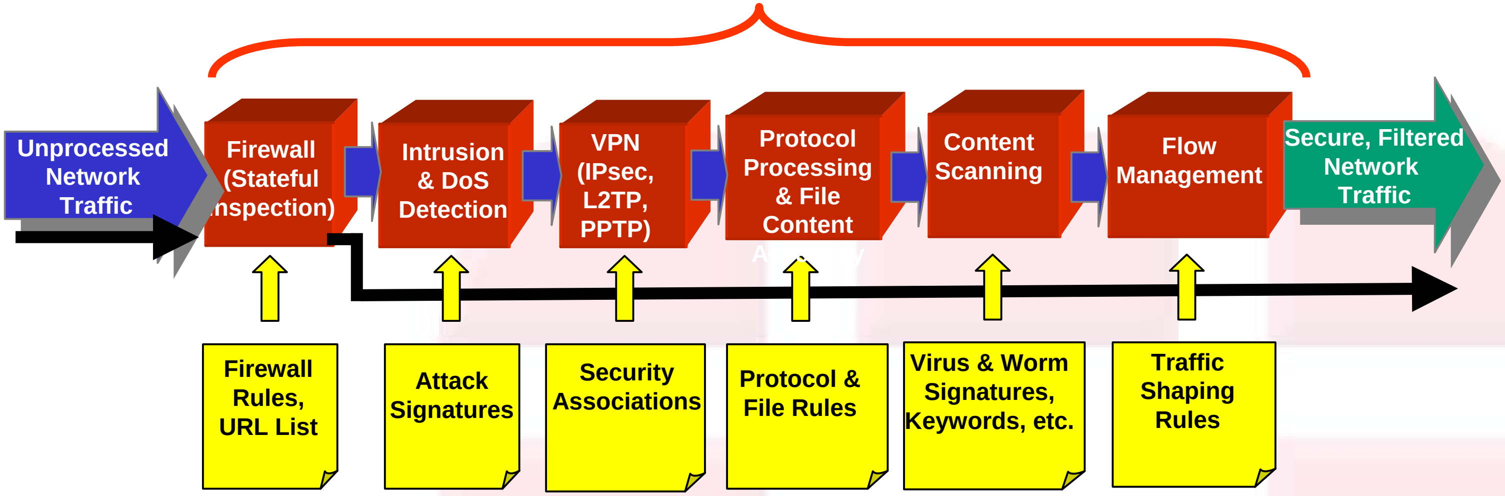


- Proprietary Fortinet Chip
- Hardware scanning engine
- Hardware encryption
- Real-time content analysis

- Real-time networking OS
- High performance
- Robust, reliable

What is the weakest point for point solution? (Why policy based management is needed ?)

FortiASIC Content Processor Chip



Unprocessed Network Traffic

Firewall (Stateful Inspection)

Intrusion & DoS Detection

VPN (IPsec, L2TP, PPTP)

Protocol Processing & File Content

Content Scanning

Flow Management

Secure, Filtered Network Traffic

Firewall Rules, URL List

Attack Signatures

Security Associations

Protocol & File Rules

Virus & Worm Signatures, Keywords, etc.

Traffic Shaping Rules

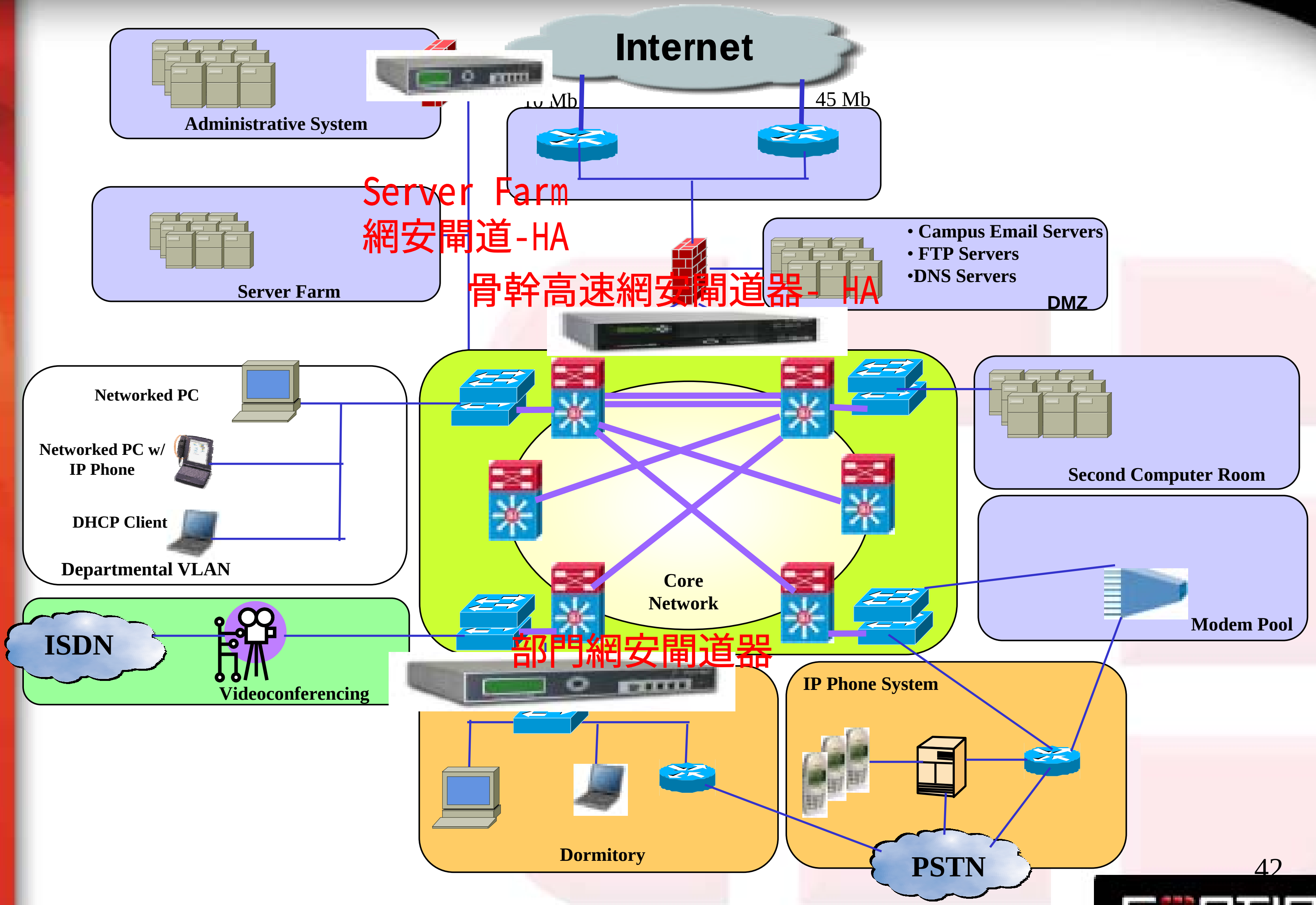
*Note: Blocks can be used in multiple combinations, e.g. firewall, AV, and other functions can be applied to decrypted VPN tunnels

FORTINET™

THE POWER IN NETWORK PROTECTION

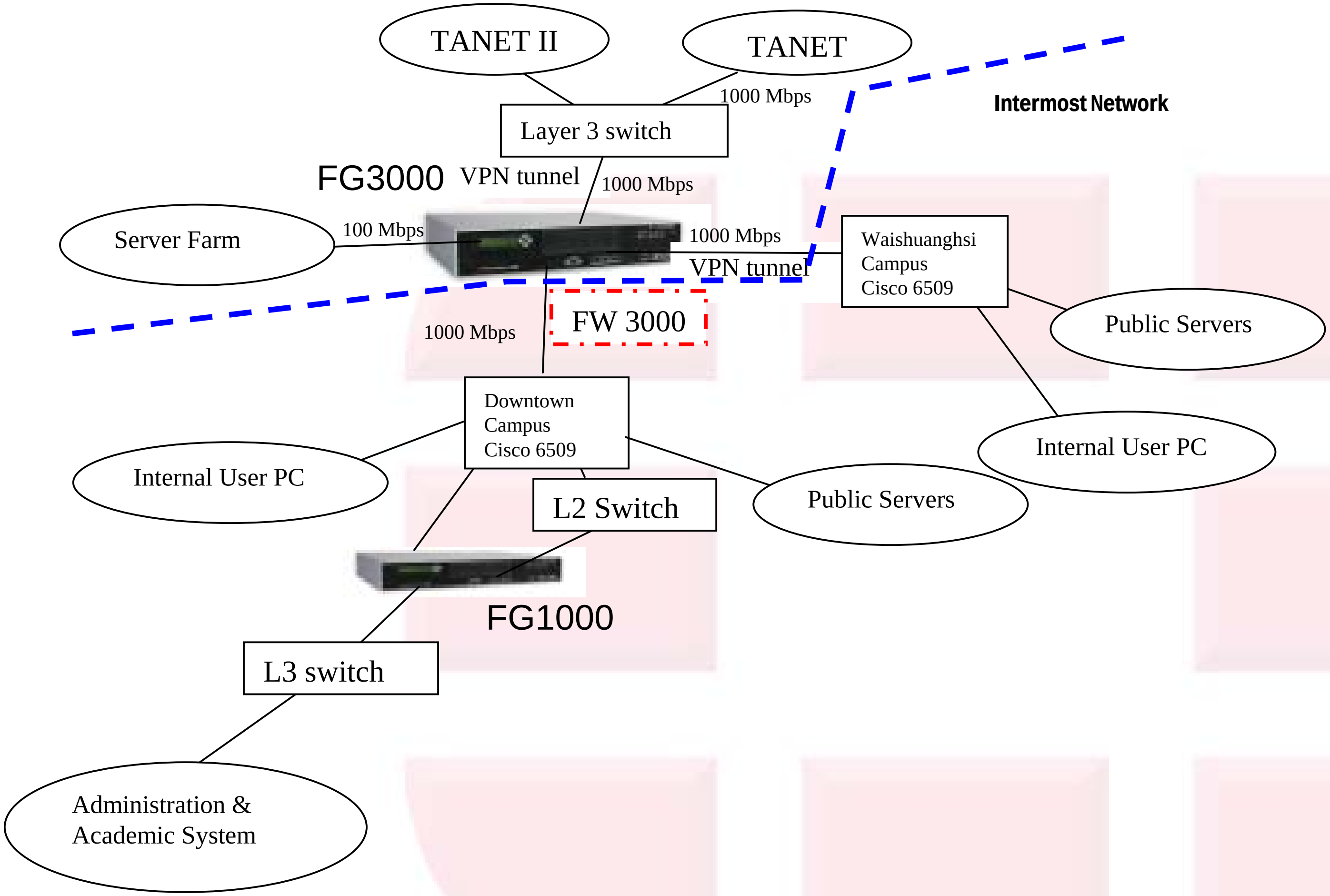
安全網路架構

FORTINET 網路安全架構圖

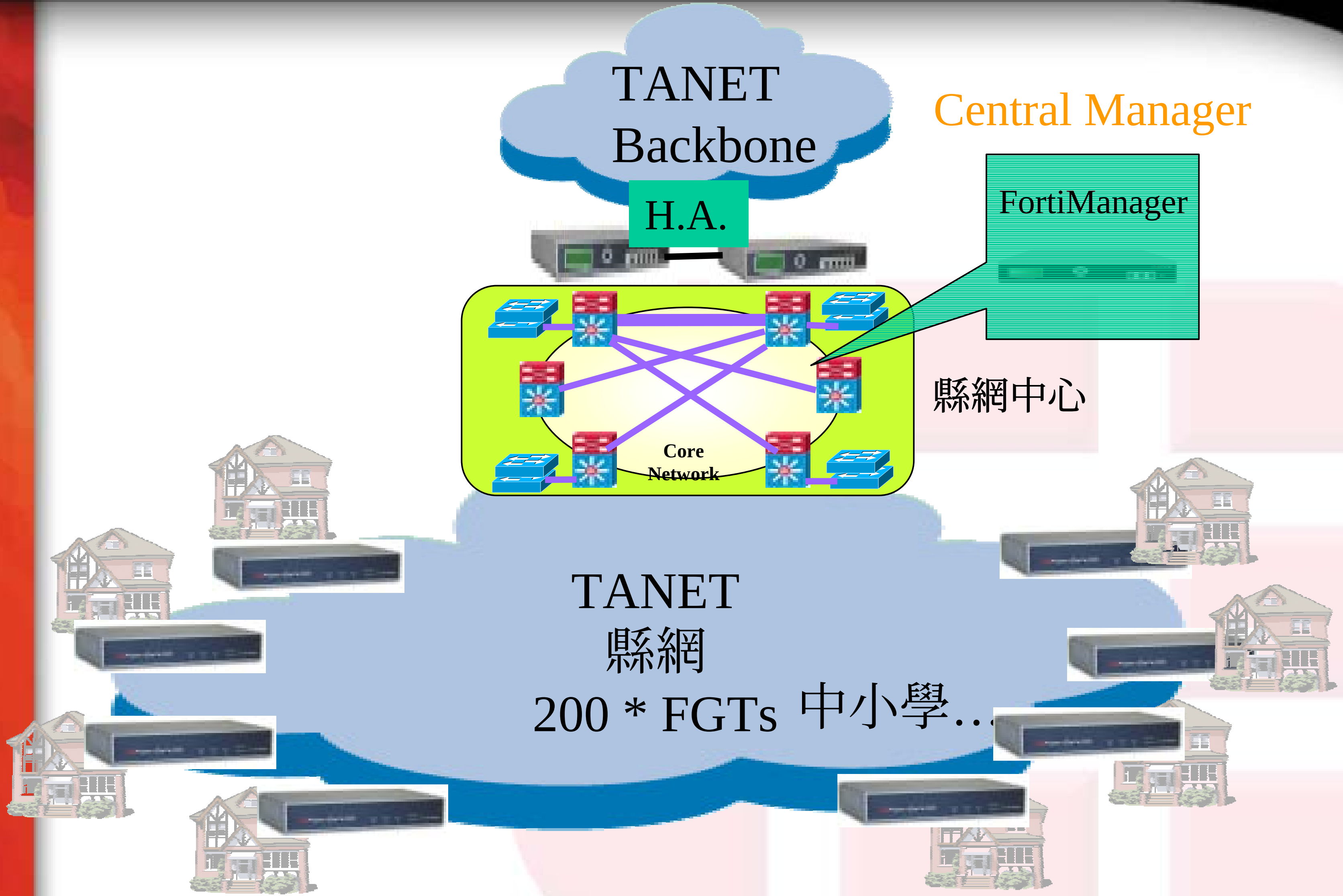


FORTINET

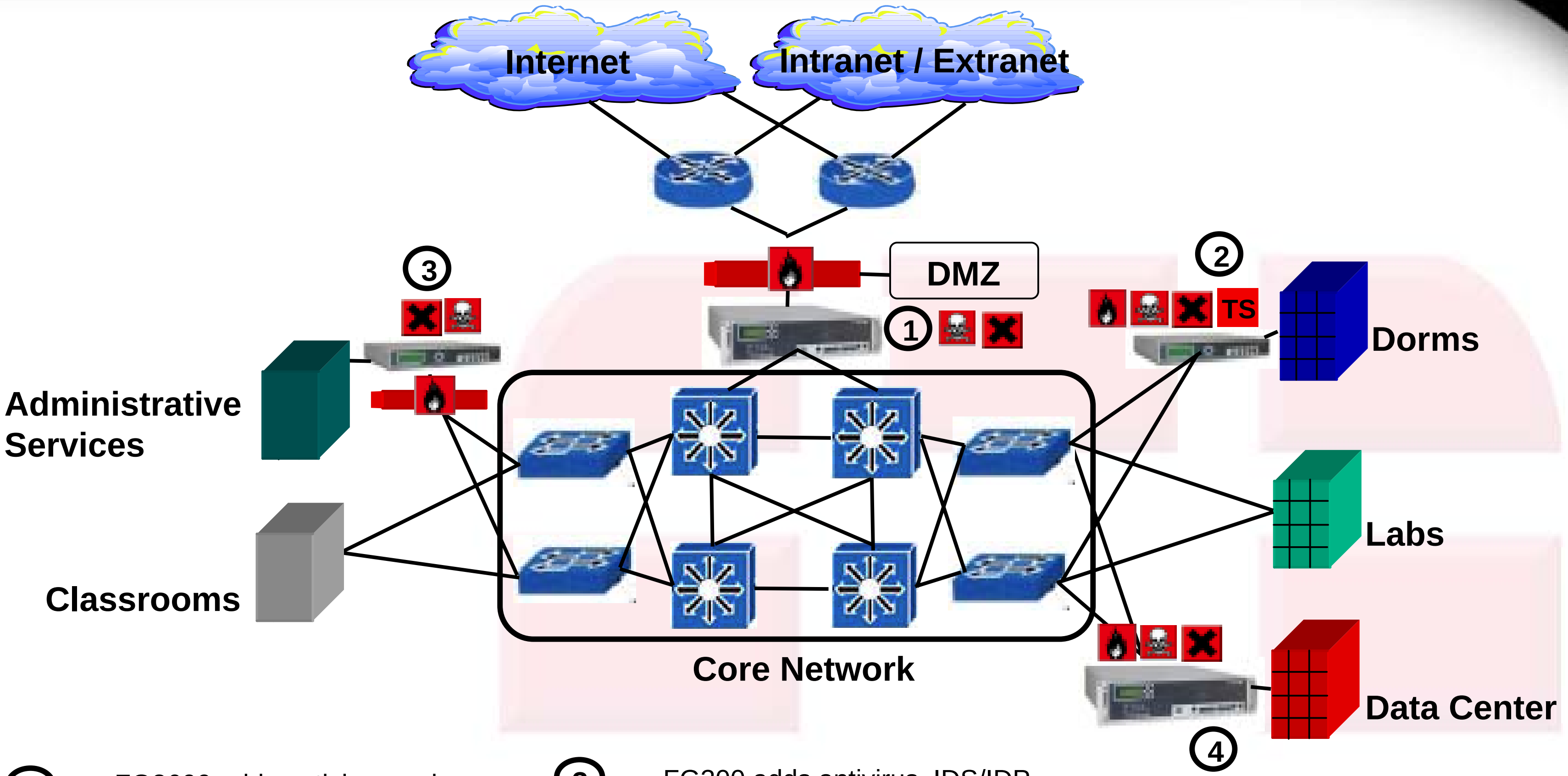
A Real Case for Education Network



Fortinet Provides a Complete Solution for the Educational Network (1/2)



Fortinet Provides a Complete Solution for the Educational Network (2/2)



1 FG3600 adds antivirus and IDS/IDP protection at the gateway in transparent mode behind existing firewall

2 FG300 provides antivirus, IDS/IDP and firewall protection, and traffic shaping functionality for dorms

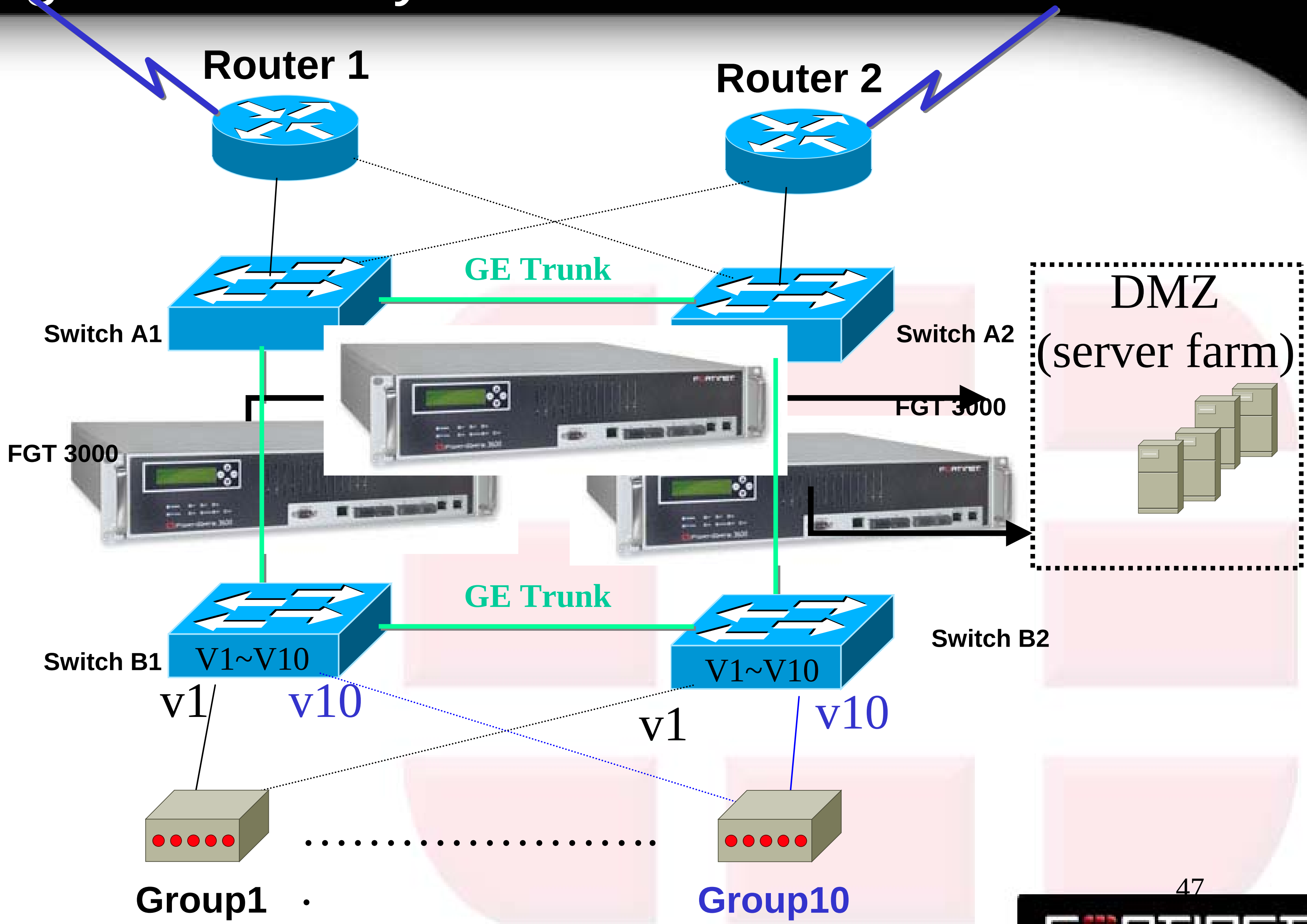
3 FG300 adds antivirus, IDS/IDP protection to exisiting firewall for administrative services

4 FG3600 provides in-line firewall, antivirus, IDS/IDP functionality to data center

High Availability Feature Highlights

- Fortigate Clustering Protocol (Real Clustering)
  Active-Active (TP / Routing mode)
  Active-Passive (TP / Routing mode)
- HA in transparent mode
- Stateful failover for both firewall and VPN traffic within 3 seconds
- Link status monitoring and failover
- HA Alert
  - During failover, the FortiGate units in an HA group send an email and SNMP trap, and log the event.

FORTINET–高可靠網路安全建議架構圖
High Availability Network Archietecture



FORTINET™

THE POWER IN NETWORK PROTECTION

Enough ?

Fortinet always think more for you

FORTINET™

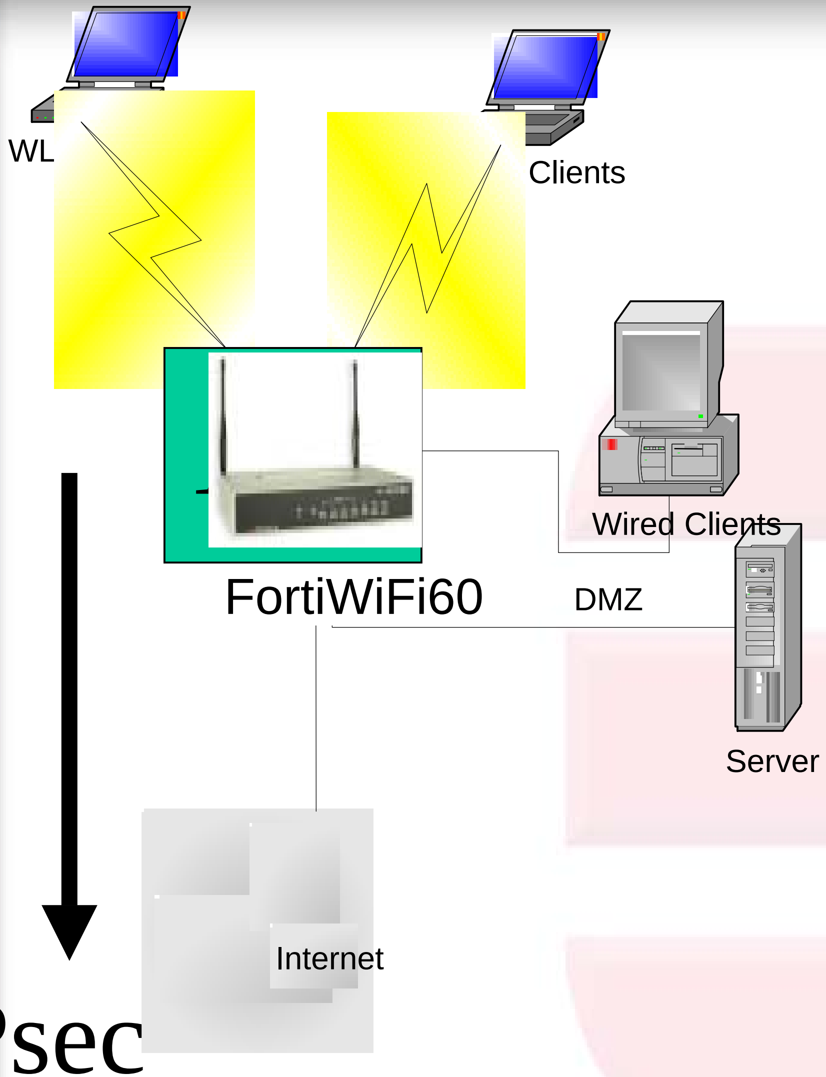
THE POWER IN NETWORK PROTECTION

無線網路安全面面觀

What is users' requirement we care ?

- **Only wireless Access Point with Compete Content Protection**

Integrated SMB Wireless Solution



IPsec

Security

- Gateway and AP not vulnerable
- AV scanning for all users at all times
- WLAN clients protected from each other
- Can enforce Security Policy at all points

- EVEN provide IPsec Tunnel directly to internet

FORTINET™

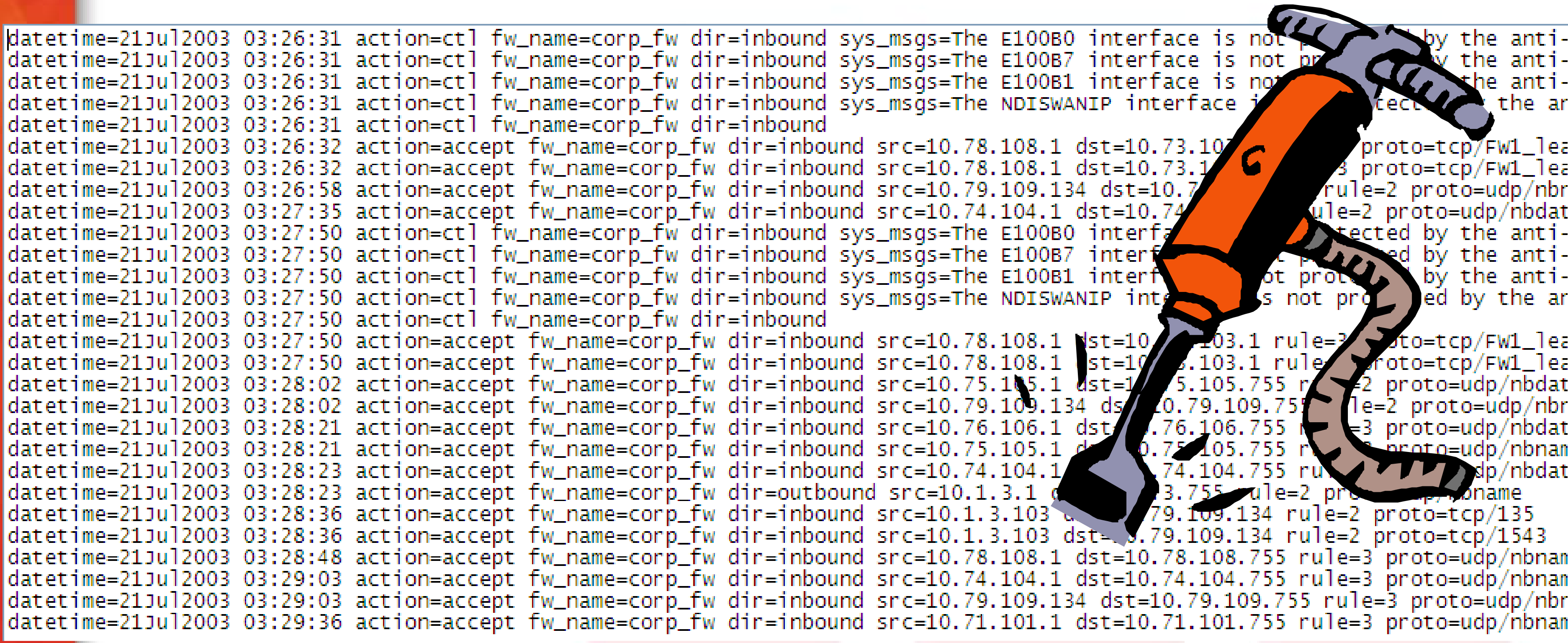
THE POWER IN NETWORK PROTECTION

Valuable Reporter is necessary

Without FirewallAnalyzer

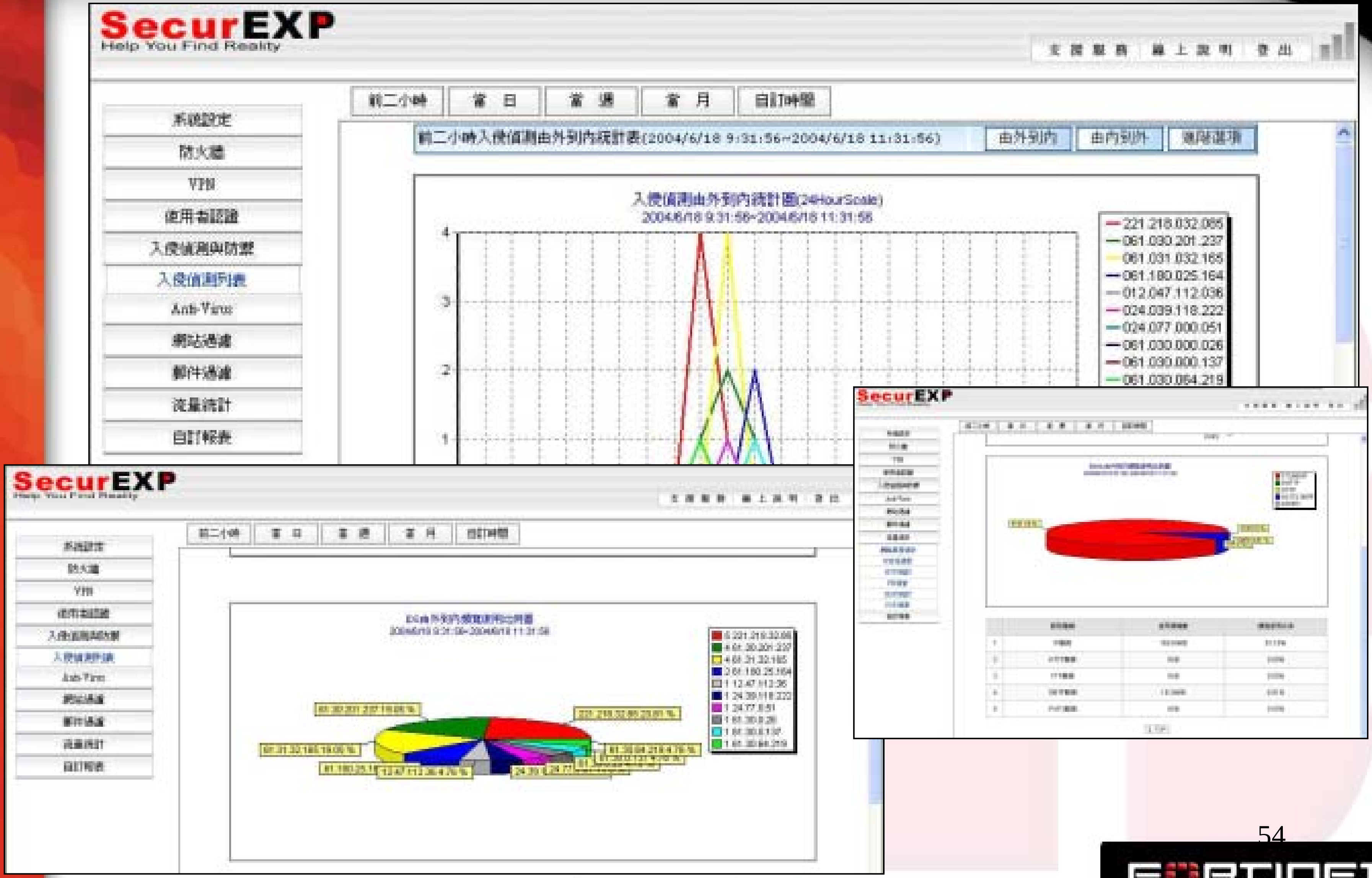
Good news is that Firewalls stream all activity in Syslog Messages. Syslog Servers capture this info into log files.

But finding valuable information in Firewall log files which contain huge amounts of cryptic information is not easy.

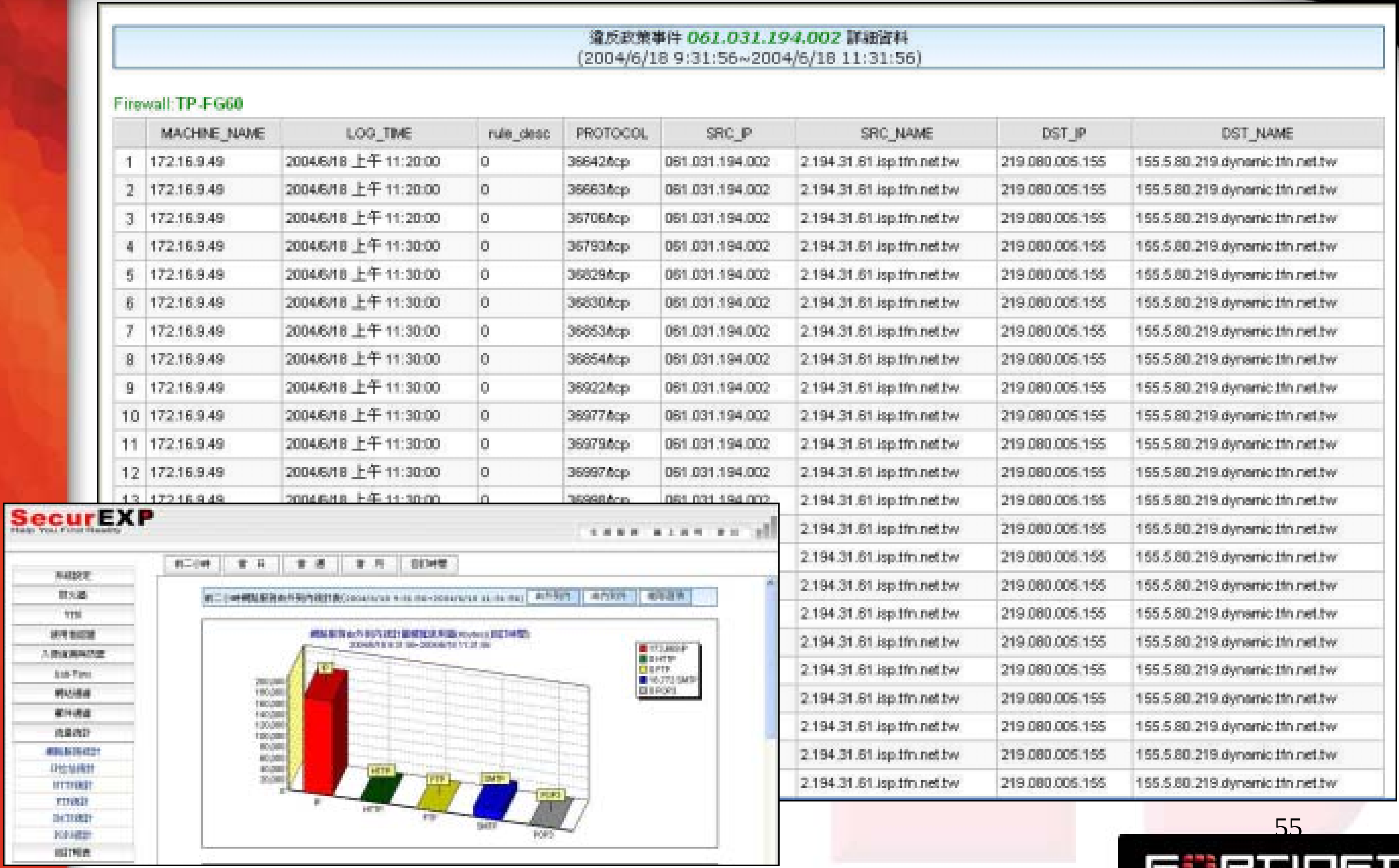


```
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B0 interface is not p        by the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B7 interface is not pr        y the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B1 interface is no           the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The NDISWANIP interface i      tect     the an
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound
datetime=21Jul2003 03:26:32 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.10         proto=tcp/FW1_lea
datetime=21Jul2003 03:26:32 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.1         3 proto=tcp/FW1_lea
datetime=21Jul2003 03:26:58 action=accept fw_name=corp_fw dir=inbound src=10.79.109.134 dst=10.7        rule=2 proto=udp/nbr
datetime=21Jul2003 03:27:35 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1 dst=10.74        ule=2 proto=udp/nbdat
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B0 interfa         tected by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B7 interf       t p    ed by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B1 interf      ot prot      by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The NDISWANIP inte      s not pro    ed by the an
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound
datetime=21Jul2003 03:27:50 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10    103.1 rule=3  oto=tcp/FW1_lea
datetime=21Jul2003 03:27:50 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 st=10  .103.1 rule  roto=tcp/FW1_lea
datetime=21Jul2003 03:28:02 action=accept fw_name=corp_fw dir=inbound src=10.75.1 5.1 dst=1  5.105.755 r  =2 proto=udp/nbdat
datetime=21Jul2003 03:28:02 action=accept fw_name=corp_fw dir=inbound src=10.79.10 .134 ds  0.79.109.755  le=2 proto=udp/nbr
datetime=21Jul2003 03:28:21 action=accept fw_name=corp_fw dir=inbound src=10.76.106.1 dst  .76.106.755 r  =3 proto=udp/nbdat
datetime=21Jul2003 03:28:21 action=accept fw_name=corp_fw dir=inbound src=10.75.105.1 d  0.7  105.755 r      proto=udp/nbnam
datetime=21Jul2003 03:28:23 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1     .74.104.755 ru          dp/nbdat
datetime=21Jul2003 03:28:23 action=accept fw_name=corp_fw dir=outbound src=10.1.3.1 d     3.755  ule=2 pr        bname
datetime=21Jul2003 03:28:36 action=accept fw_name=corp_fw dir=inbound src=10.1.3.103      79.109.134 rule=2 proto=tcp/135
datetime=21Jul2003 03:28:36 action=accept fw_name=corp_fw dir=inbound src=10.1.3.103 dst-  .79.109.134 rule=2 proto=tcp/1543
datetime=21Jul2003 03:28:48 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.78.108.755 rule=3 proto=udp/nbnam
datetime=21Jul2003 03:29:03 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1 dst=10.74.104.755 rule=3 proto=udp/nbnam
datetime=21Jul2003 03:29:03 action=accept fw_name=corp_fw dir=inbound src=10.79.109.134 dst=10.79.109.755 rule=3 proto=udp/nbr
datetime=21Jul2003 03:29:36 action=accept fw_name=corp_fw dir=inbound src=10.71.101.1 dst=10.71.101.755 rule=3 proto=udp/nbnam
```

FirewallAnalyzer – Instant Reporting



FirewallAnalyzer – Drill Down



違反政策事件 061.031.194.002 詳細資料
(2004/6/18 9:31:56~2004/6/18 11:31:56)

Firewall:TP-FG60

	MACHINE_NAME	LOG_TIME	rule_desc	PROTOCOL	SRC_IP	SRC_NAME	DST_IP	DST_NAME
1	172.16.9.49	2004/6/18 上午 11:20:00	0	36642/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
2	172.16.9.49	2004/6/18 上午 11:20:00	0	36663/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
3	172.16.9.49	2004/6/18 上午 11:20:00	0	36706/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
4	172.16.9.49	2004/6/18 上午 11:30:00	0	36793/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
5	172.16.9.49	2004/6/18 上午 11:30:00	0	36829/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
6	172.16.9.49	2004/6/18 上午 11:30:00	0	36830/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
7	172.16.9.49	2004/6/18 上午 11:30:00	0	36853/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
8	172.16.9.49	2004/6/18 上午 11:30:00	0	36854/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
9	172.16.9.49	2004/6/18 上午 11:30:00	0	36922/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
10	172.16.9.49	2004/6/18 上午 11:30:00	0	36977/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
11	172.16.9.49	2004/6/18 上午 11:30:00	0	36979/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
12	172.16.9.49	2004/6/18 上午 11:30:00	0	36997/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
13	172.16.9.49	2004/6/18 上午 11:30:00	0	36998/tcp	061.031.194.002	2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw
						2.194.31.61.isp.tfn.net.tw	219.080.005.155	155.5.80.219.dynamic.tfn.net.tw