ITALTEL
Roots to the future

infosecurity
ITALIA
11-13 FEBBRAIO 2004
FIERA MILANO
www.infosecurity.it

Attacchi DDoS: le contromisure a carico dei Service Provider e quelle a carico delle Imprese

Maurizio Tondi
Direttore Marketing Professional Services

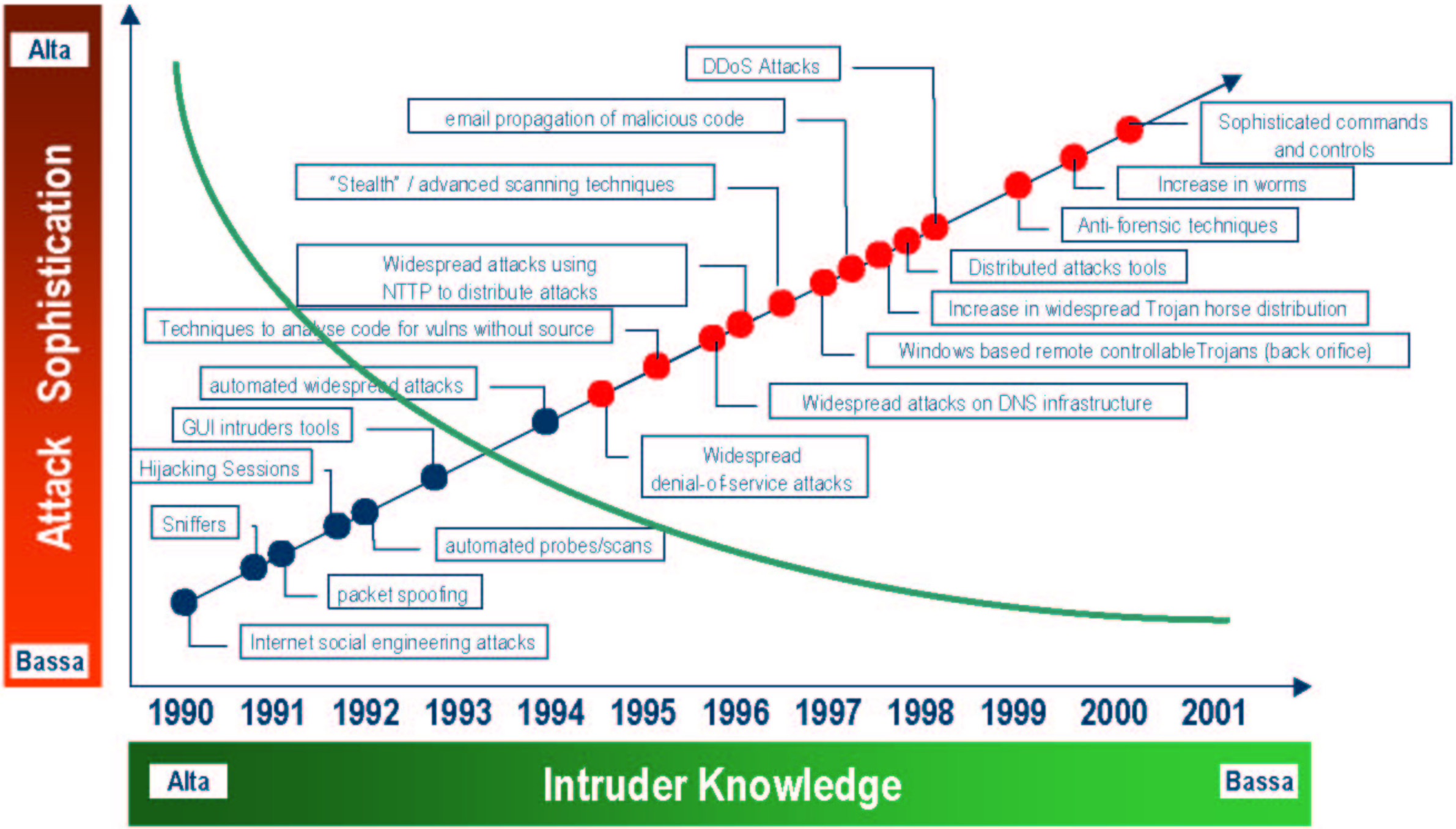
Infosecurity 2004

EVOLUZIONE DELLE MINACCE ALLA SICUREZZA INFORMATICA

Negli ultimi anni si sono verificate le seguenti tendenze:

1- L'expertise necessaria per attuare attacchi alla sicurezza informatica si è ridotta

2- Gli attacchi informatici sono diventati molto più sofisticati



Source: CERT / Carnegie Mellon University 1998-2003

EVOLUZIONE DELLA STRATEGIA DENIAL-OF-SERVICE

DRDoS

il DRDoS (**Distributed Reflection Denial of Service**) è l'attuazione di un DDoS con una ulteriore moltiplicazione delle fonti d'attacco e avviene mediante il reclutamento di high bandwidth internet server i*nconsapevoli,* innescati da SYN packets (richieste di connnessione). Tali server diventano "riflettenti" immettendo in rete un numero elevatissimo di pacchetti SYN/ACK diretti verso la vittima.

DDoS

il DDoS **(Distributed Denial of Service)** è l'attuazione di un DOS mediante la moltiplicazione delle fonti d'attacco (anche centinaia di migliaia di computer). Si attua attraverso un mass-mailing worm che infetta i computer, aprendo una backdoor attraverso cui l'hacker può connettersi al computer e impiegare le sue risorse. Il DDoS ha lo scopo di saturare sia le risorse dell'obiettivo che quelle delle reti.

DoS

il DOS (**Denial of Service**) è l'attacco a un server (web, mail, DNS, etc.), attuato mediante l'invio di un'elevata quantità di pacchetti ad alta velocità. Il DOS ha lo scopo di saturare le risorse dell'obiettivo rendendolo inutilizzabile durante l'attacco.

I PRINCIPALI ATTACCHI DDoS NEL MONDO

2001

- **Microsoft**
  (perdite pari a 500 milioni$)

2002

- **Amazon**
- **Yahoo**
- **eBay**
- **CNN, etc.**

Perdite cumulative pari a 1,2 miliardi $ (Yankee Group)

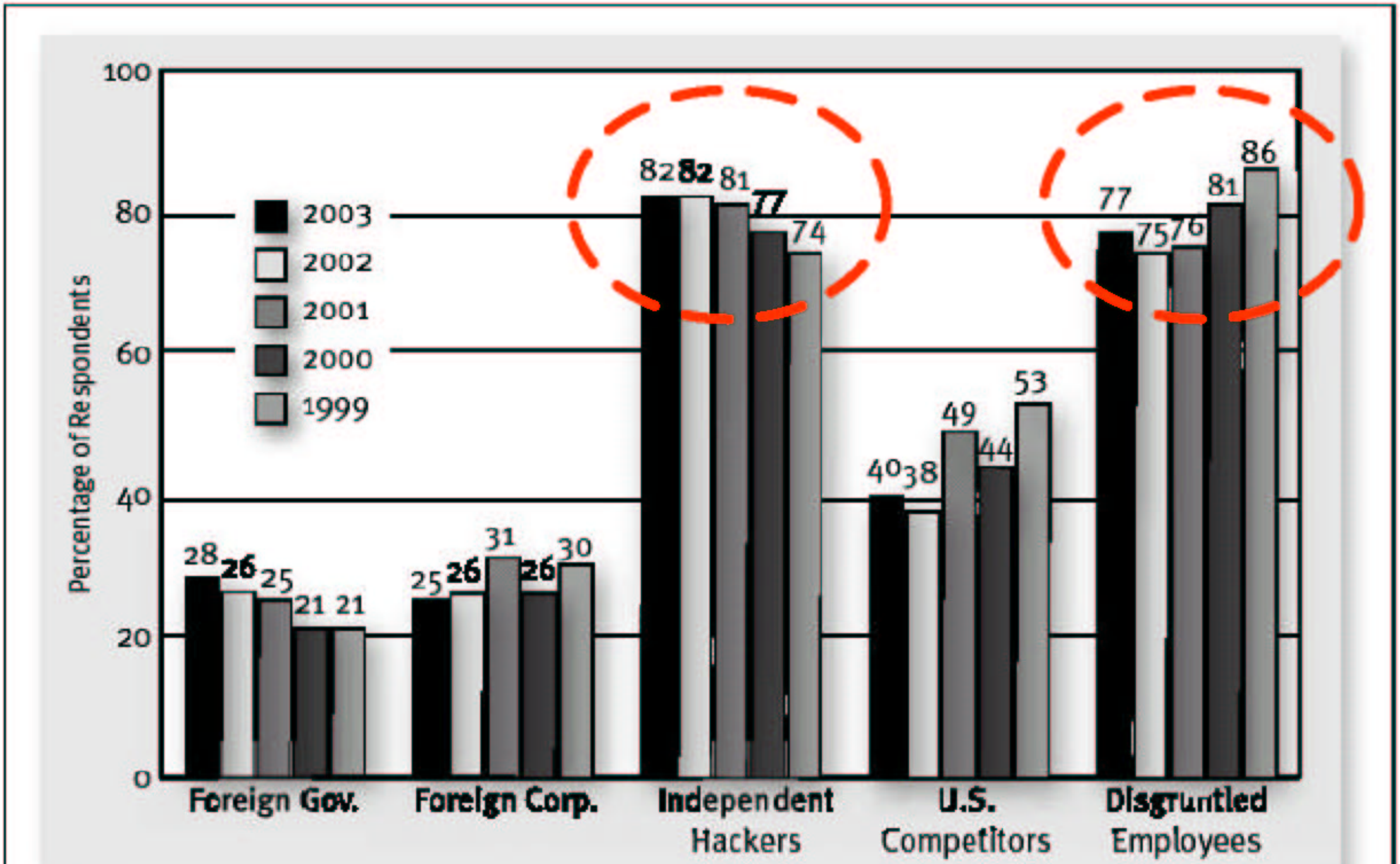
2003

- **Microsoft**
  (worm SQL Slammer)
- **Bank of America**
- **Continental Airlines**
- **Poste Italiane**
  14.000 terminali bloccati per 4h
- **Pakistan Governement**
- **Al-Jazeera Qatar TV**

2004

- **Microsoft**
- **SCO**
  (worm Mydoom)
- .....
- .....
- .....

LE FONTI DEGLI ATTACCHI SECONDO FBI



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 488 Respondents/92%
2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%

5 Febbraio 2004 08:49 - INTERNET: MYDOOM, 48.000 PC COLPITI IN ITALIA IN 7 GIORNI

(ANSA) - ROMA, 5 FEB - Sono stati circa 48.000 i computer colpiti dal virus MyDoom in Italia nell'ultima settimana, quasi 1.390 nelle ultime 24 ore. Nel mondo sono stati complessivamente oltre 800.000 i computer danneggiati, dagli Stati Uniti alla Cina, e il sito dell'azienda americana SCO crollato sotto il peso di 2,5 milioni richieste di connessione in meno di 12 ore. Il numero dei computer colpiti finora sembra non avere precedenti, rilevano gli esperti dell'azienda specializzata in sicurezza informatica Trend Micro, ma al momento e' impossibile fare una stima dei danni. Sempre secondo l'azienda, l'epidemia oggi sembra dare i primi segni di rallentamento, ma continua ad essere allarme giallo a livello internazionale. MyDoom, noto anche come Mimail o Novarg.A, e' stato infatti progettato per lanciare i suoi attacchi ai siti delle aziende americane SCO (dalla prima versione in circolazione, MyDoom.A) e Microsoft (dalla seconda

5 Febbraio 2004 08:49 - INTERNET: MYDOOM, 48.000 PC COLPITI IN ITALIA IN 7 GIORNI

(ANSA) - ROMA, 5 FEB - Sono stati circa 48.000 i computer colpiti dal virus MyDoom in Italia nell'ultima settimana, quasi 1.390 nelle ultime 24 ore. Nel mondo sono stati complessivamente oltre 800.000 i computer danneggiati, dagli Stati Uniti alla Cina, e il sito dell'azienda americana SCO crollato sotto il peso di 2,5 milioni richieste di connessione in meno di 12 ore. Il numero dei computer colpiti finora sembra non avere precedenti, rilevano gli esperti dell'azienda specializzata in sicurezza informatica Trend Micro, ma al momento e' impossibile fare una stima dei danni. Sempre secondo l'azienda, l'epidemia oggi sembra dare i primi segni di rallentamento, ma continua ad essere allarme giallo a livello internazionale. MyDoom, noto anche come Mimail o Novarg.A, e' stato infatti progettato per lanciare i suoi attacchi ai siti delle aziende americane SCO (dalla prima versione in circolazione, MyDoom.A) e Microsoft (dalla seconda versione, MyDoom.B) ancora per otto giorni, fino al 12 febbraio Come tanti altri programmi pericolosi, MyDoom ha provocato parecchi fastidi, sovraccaricando la posta elettronica di messaggi e rallentando i sistemi operativi. Rispetto ai suoi predecessori si comporta pero' in modo anomalo. MyDoom e' infatti un virus furbo: sembra essersi diffuso in modo da evitare siti nei quali sarebbe stato facilmente rintracciabile, come quelli di aziende specializzate in sicurezza informatica, della Pubblica amministrazione e di enti governativi, ha osservato Tiberio Molino, della Trend Micro Italia. Una delle ipotesi piu' accreditate tra gli esperti, e' che MyDoom sia stato progettato cosi' proprio per avere maggiori probabilita' di successo nel "reclutare" il maggior numero possibile di computer per raggiungere l'obiettivo finale: l'attacco ai siti di SCO e Microsoft. Ecco allora le tre caratteristiche che gli permettono di diffondersi: - E' UN VIRUS: si diffonde producendo numerose copie di se'; - E' UN WORM: si propaga da un computer all'altro utilizzando una rete informatica; - E' UN CAVALLO DI TROIA: raggiunge i computer degli utenti mascherato, inducendoli a trattarlo come un messaggio di e-mail legittimo. - EVITA HACKER E SITI GOVERNATIVI: chi ha programmato MyDoom ha istruito il virus in modo da non fargli colpire gli altri hacker. Gli ha inoltre insegnato a non attaccare gli utenti di Linux, i militari e le istituzioni governative. - INGEGNERIA SOCIALE: gli americani chiamano cosi' la tecnica tipica degli hacker che punta a guadagnarsi la fiducia degli utenti, spingendoli a superare eventuali esitazioni nell'aprire un messaggio di posta elettronica. MyDoom appare infatti nella casella di posta come un messaggio assolutamente credibile.(ANSA).

MODALITA' DI UN ATTACCO DDoS (FASE I)

'Zombies'

AS

HACKER

AS

FASE I

Mass-mailing worms: PC & Server Innocenti si trasformano in *'Zombies'*

Peering Point

ISP Backbone

Web server

attacked server

VITTIMA

AS

ombies'

DNS

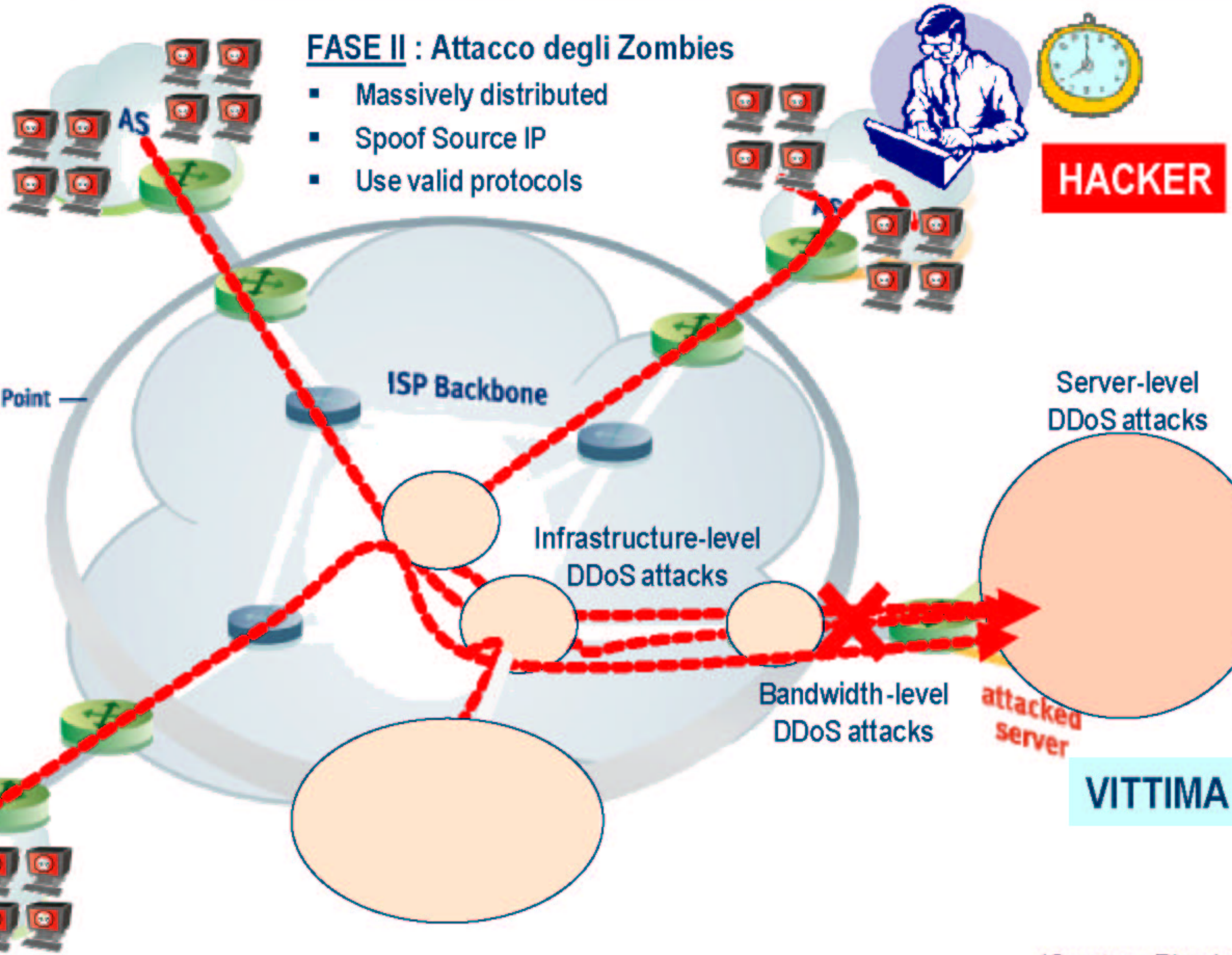
Email

(Courtesy Riverhead)

CONSEGUENZE DI UN ATTACCO DDoS (FASE II)

FASE II : Attacco degli Zombies

- Massively distributed
- Spoof Source IP
- Use valid protocols



(Courtesy Riverhead)

DEVIAZIONE E PULIZIA DEL TRAFFICO INFETTO

5. Invio del traffico "ripulito" alla vittima

4. Filtraggio del traffico infetto

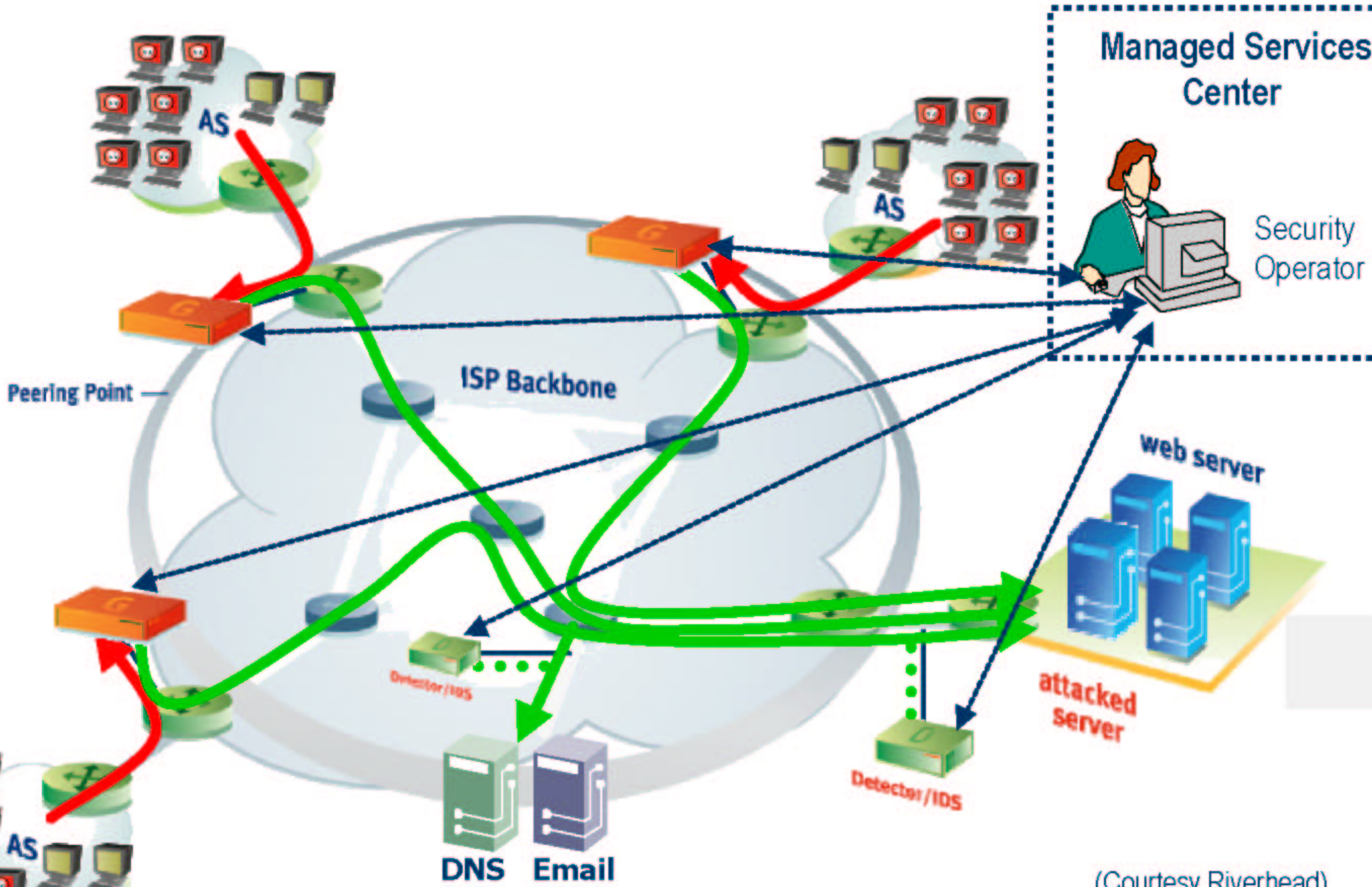
3. Deviazione solo del traffico della vittima

2. Attivazione

1. Rilevazione

(Courtesy Riverhead)

SOLUZIONE PER SERVICE PROVIDER



(Courtesy Riverhead)

Managed Services Center

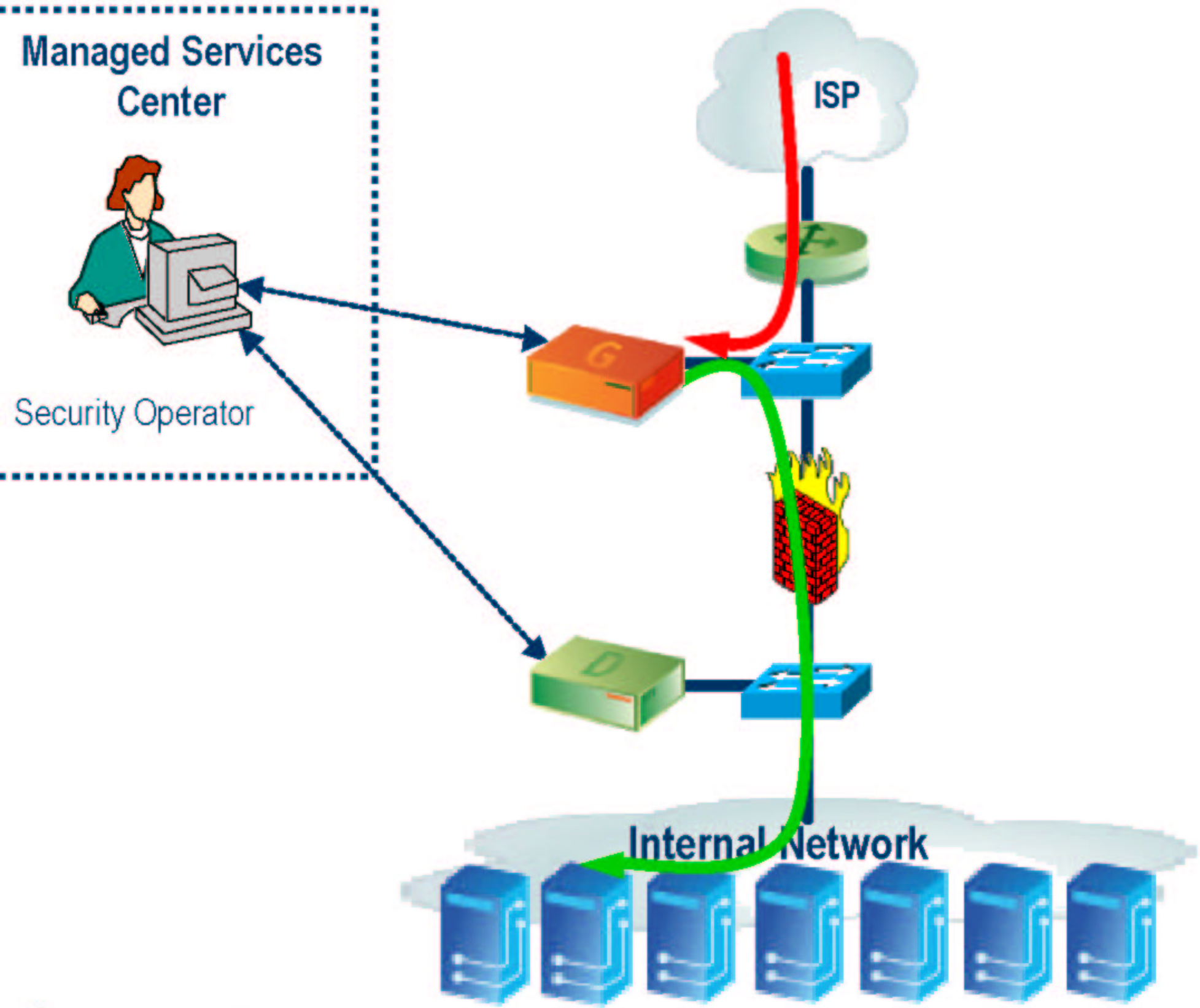
Security Operator

ISP A

ISP B

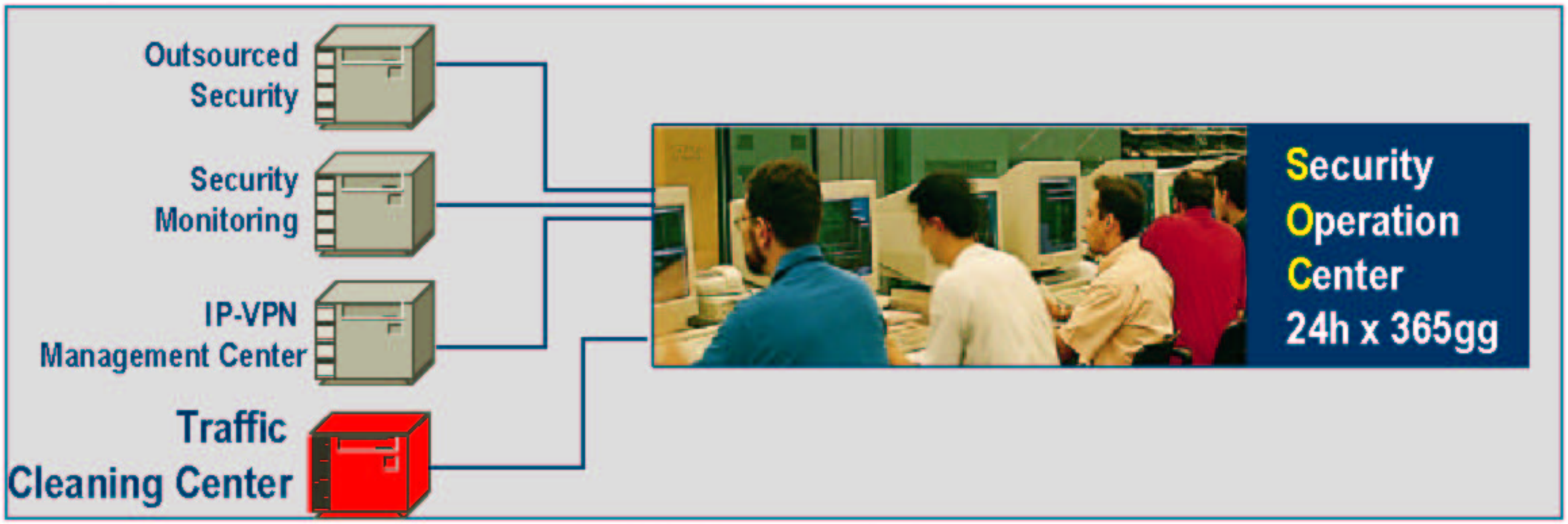
Internal Network

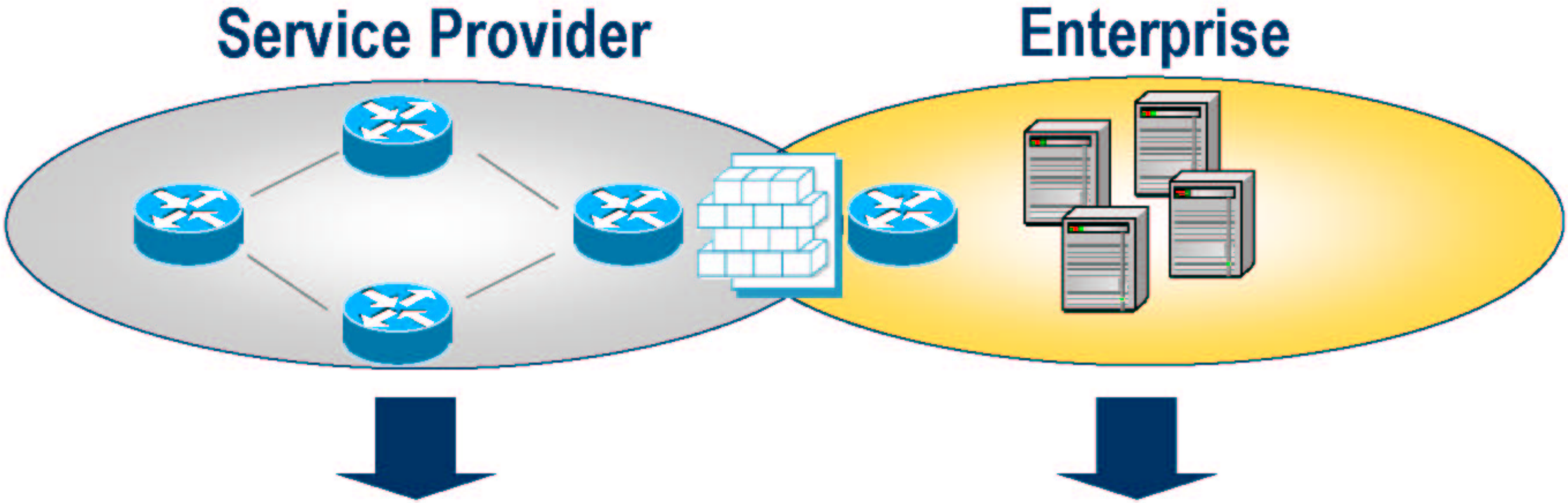
(Courtesy Riverhead)



(Courtesy Riverhead)

"CARRIER CLASS" SECURITY OPERATION CENTER





Valutazione del Livello di rischio
ROI
Benefici ottenibili

Grazie per l'attenzione

maurizio.tondi@italtel.it