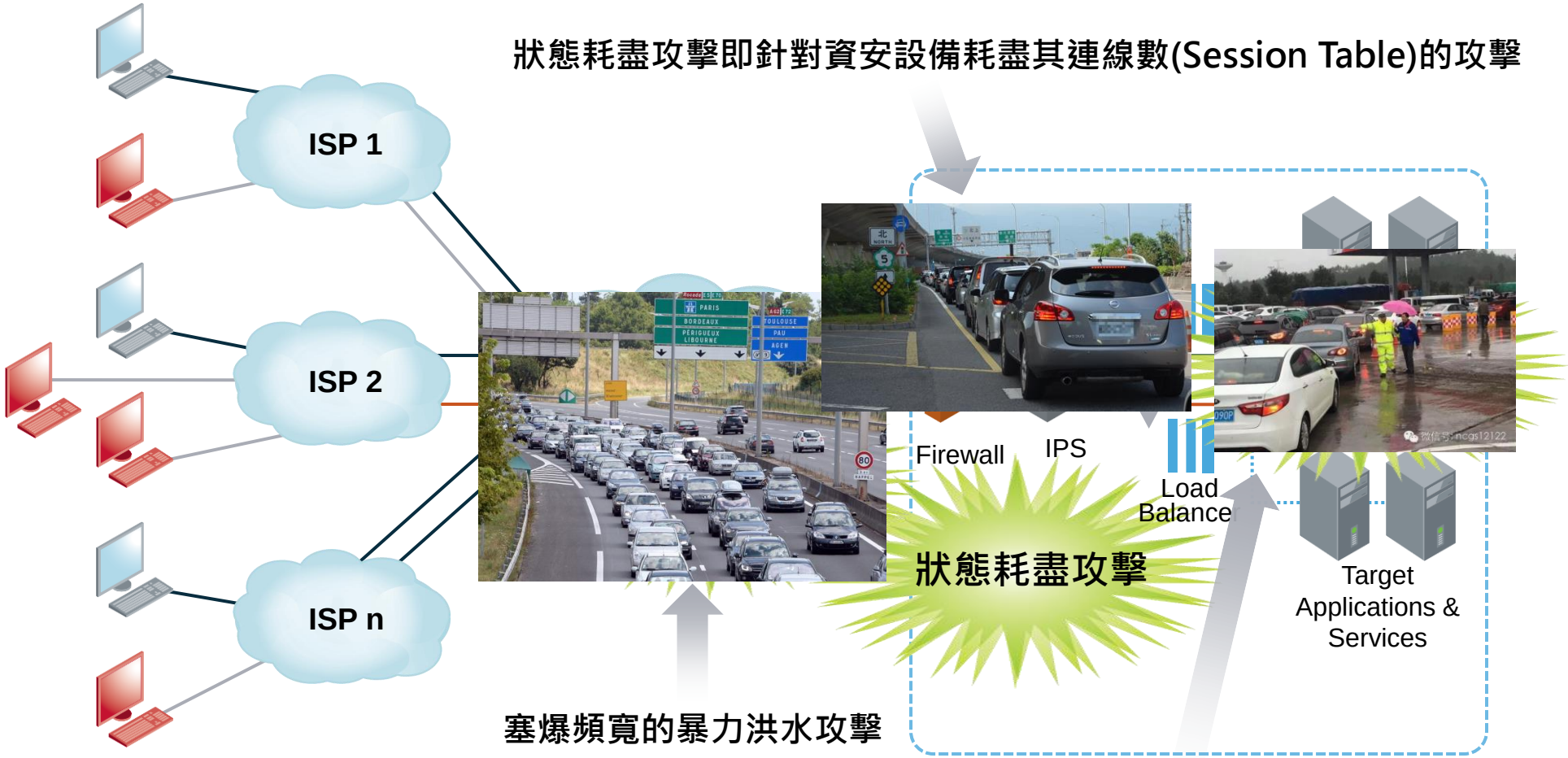
ARBOR NETWORKS
The Security Division of NETSCOUT

新型態校園資安威脅

Arbor Networks
Alex Chin
Managing Director, Greater China
achin@arbor.net

金大剛
大中華區, 總經理

DDoS攻擊型態分類

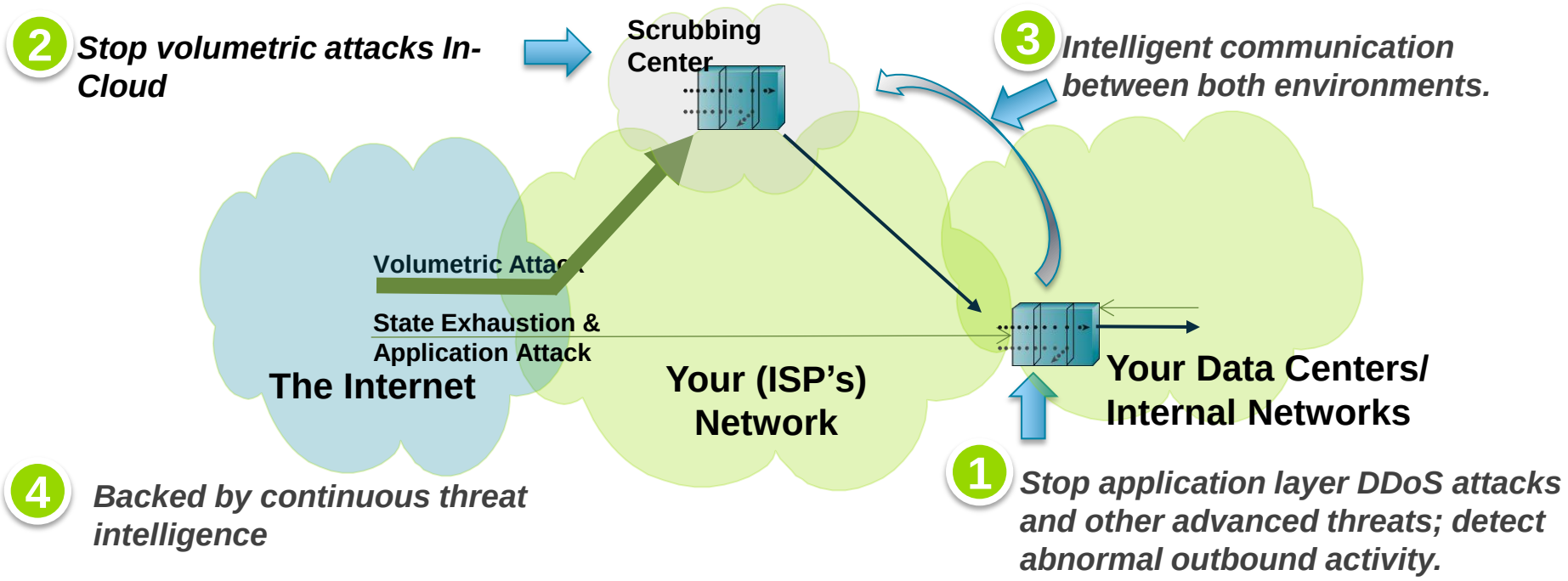


各大DDoS防護門派

- FW/IPS/WAF/LB + DDoS防護
- 當地電信業者/國際流量清洗中心
- CDN業者

專家建議: 如何有效防御DDoS攻擊

階層式DDoS防護政策

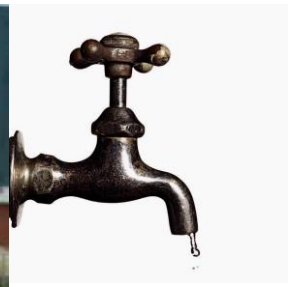


Gartner FROST & SULLIVAN IDC Analyze the Future Infonetics RESEARCH FORRESTER Securosis ovum

To defend against complex, application-based attacks, a mis of local protection (on-premises DDoS applicances) and mitigation services is a strong option.

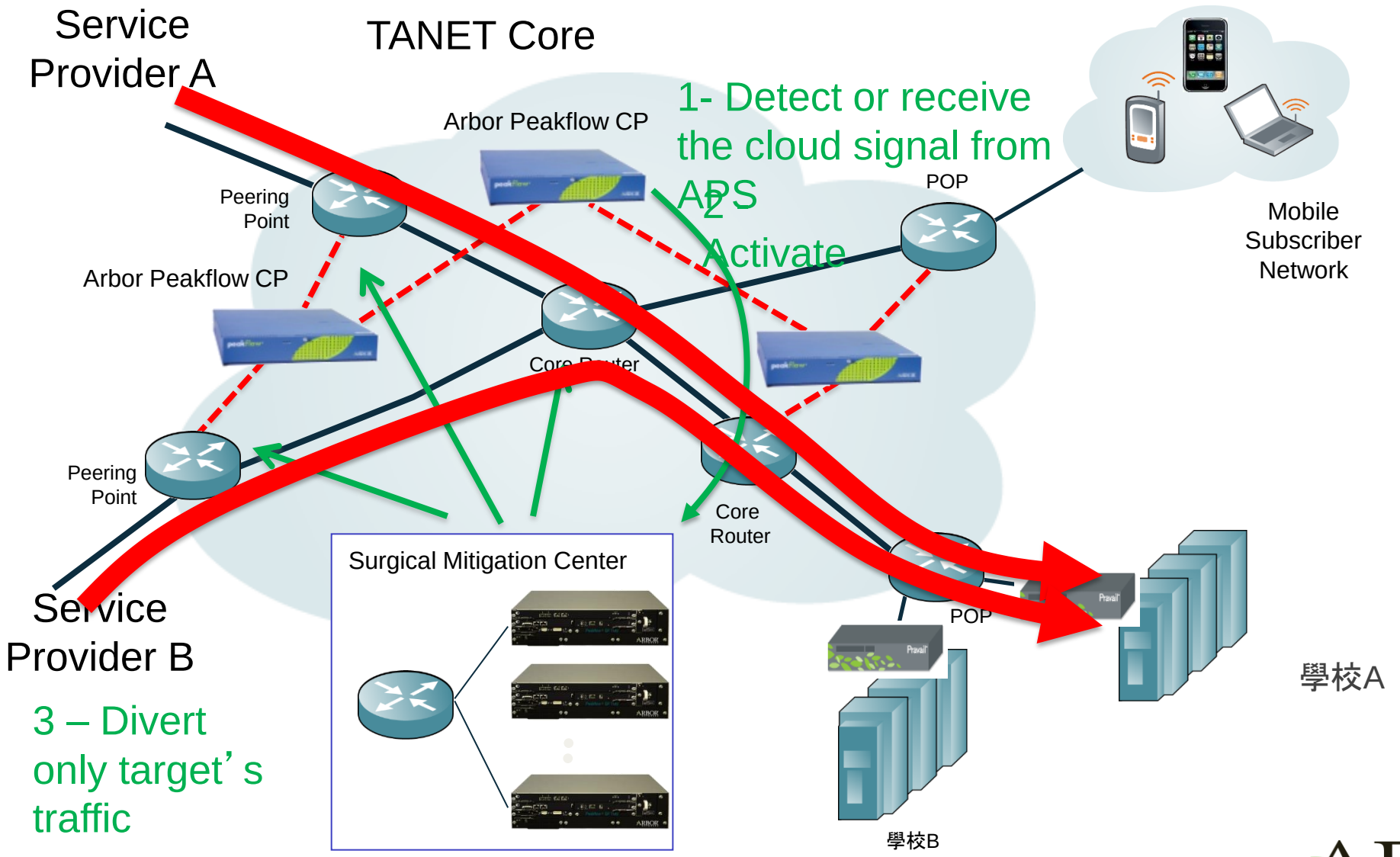
ARBOR NETWORKS

自來水廠 vs. 家用濾水器



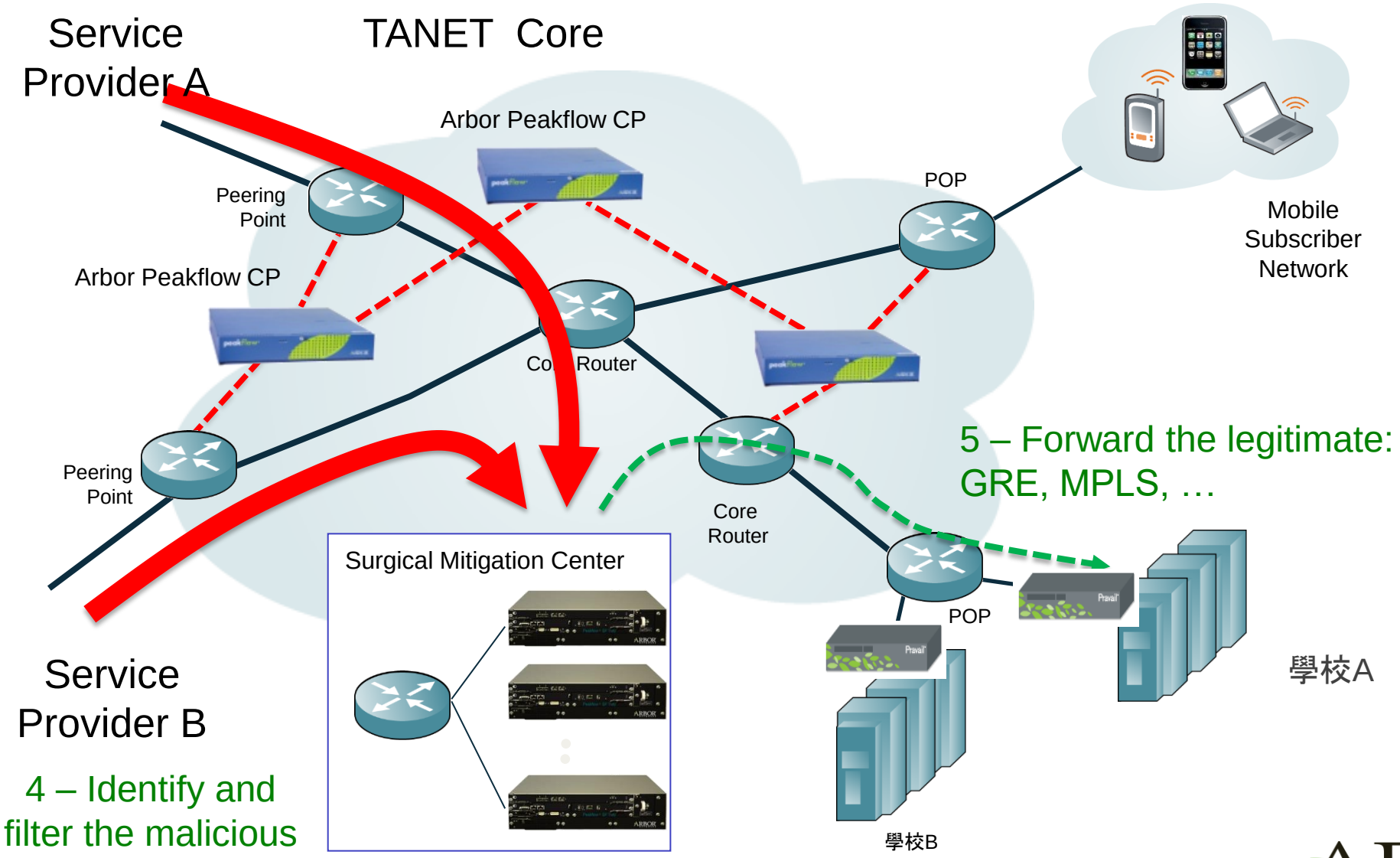
階層式DDoS防護政策(骨幹端):

Peakflow SP (Service Provider)

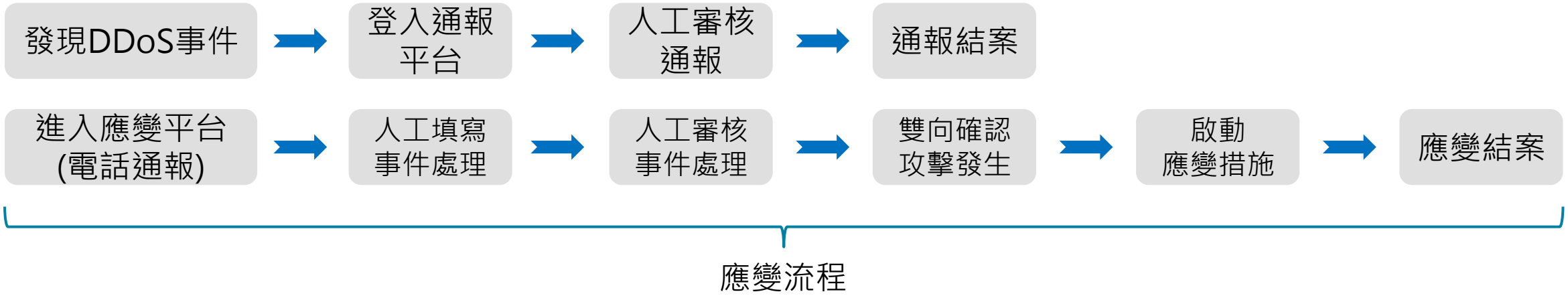


階層式DDoS防護政策(骨幹端):

Peakflow SP (Service Provider)

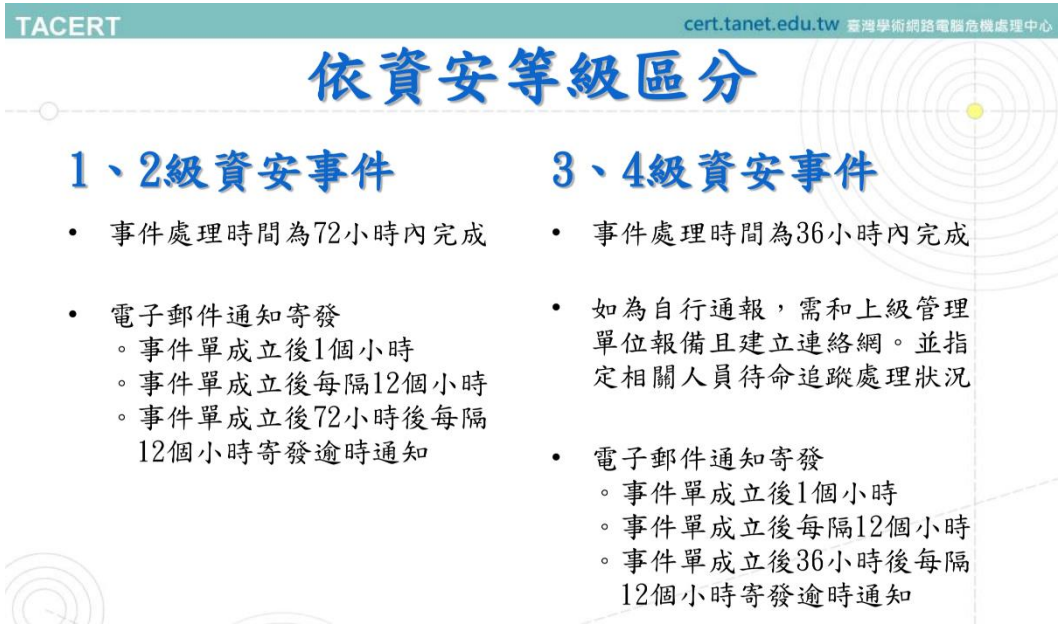


目前TANET DDoS攻擊對應流程



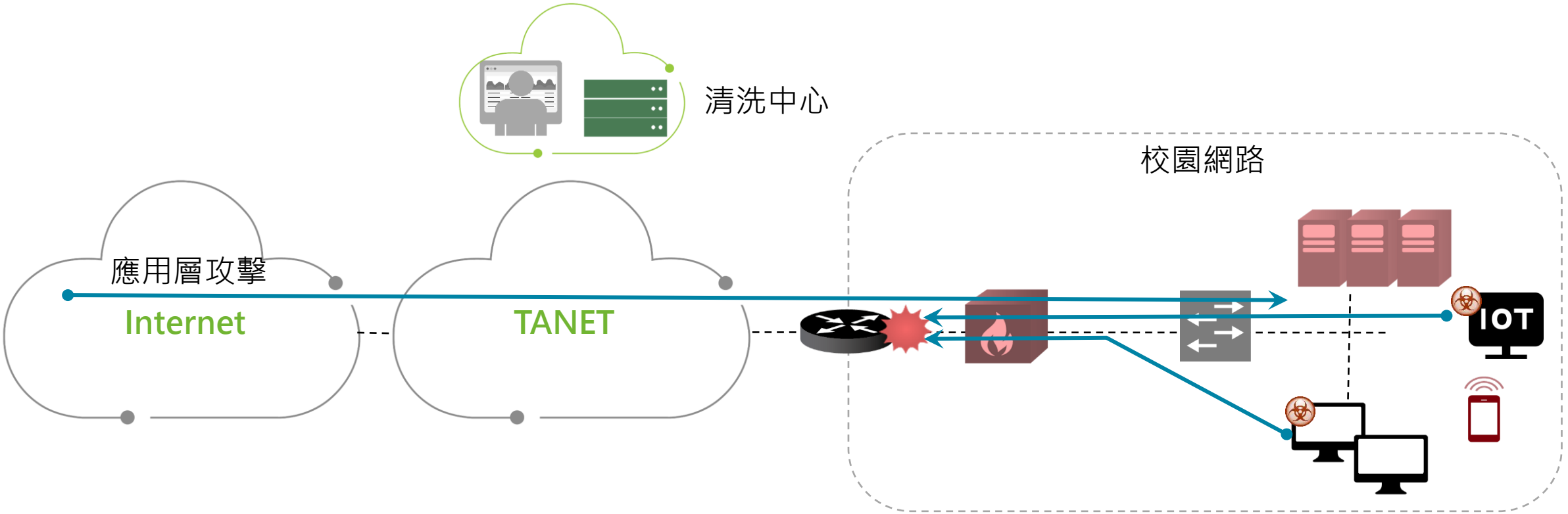
- 審核與應變過程需花費至少一小時才能完成
- 應變起始到結案需人工確認才啟動清洗機制
- 清洗設備需位於網路骨幹中，處理流量過大無法針對Layer7流量進行防禦

如果沒有Always on的即時偵測及快速清洗機制, 目前的通報及應變流程將緩不濟急.



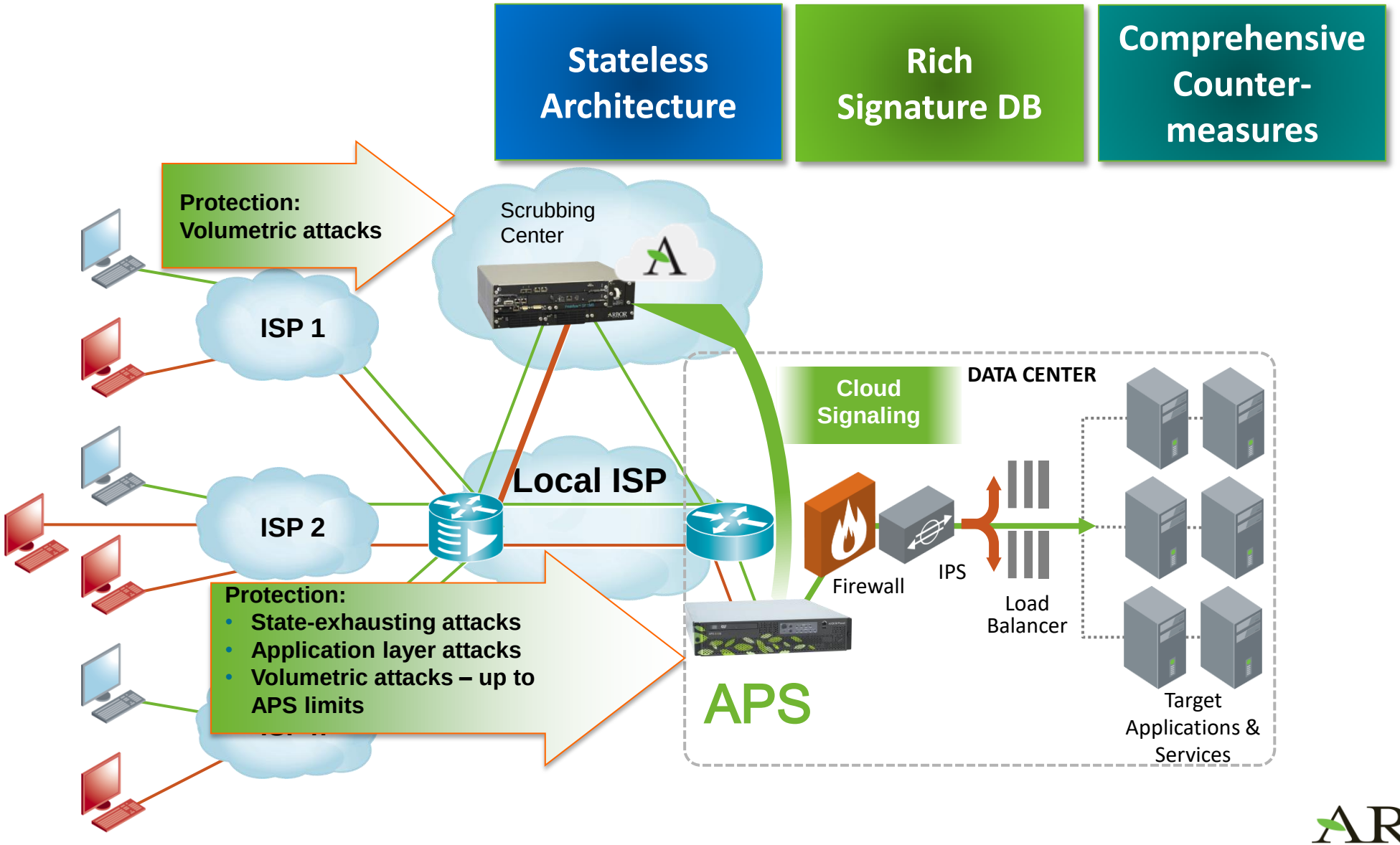
目前DDoS攻擊對應流程

- 無法主動偵測並即時攔截外對內的攻擊
- 清洗中心無法防止來自校園內部的攻擊
- 校園缺少內到外連線阻斷與DDoS防禦機制



階層式DDoS防護政策(骨幹端):

APS (Availibility Protection System)



預防勝於治療

DDoS 攻擊只靠雲端自來水廠清洗?!

加裝客製化濾水器才是王道

鄭惠如／台北

DDoS分散式阻斷服務攻擊，近年來不僅日益複雜，同時更經常搭配DNS反射／放大等更趨複雜兇猛的攻勢，再度成爲令各行各業聞之色變的資安威脅。爲此，多數企業或網際網路服務供應商(ISP)，開始大幅倚重雲端清洗中心，然而，這就足以正確擋阻DDoS嗎？！

專業二類電信服務商暉捷科技，以提供主機代管、網路服務爲主要服務，公司登記於台中，迄今已累積可觀用戶群。在更趨複雜、多變的網路環境下，近年來爲保護客戶數位資產，對於強化資訊服務管理與安全服務不遺餘力，面臨更複雜、流量更大的DDoS攻擊，也費心在專家的建議下，採購流量清洗中心、雲端服務及次世代防火牆等多層防禦機制，希望能有效阻擋DDoS。

暉捷總經理魏榮村指出，原以爲憑藉流量清洗中心，即能有效過濾去除大部分攻擊流量，剩餘殘存惡意流量，倚靠高規格防火牆便可清除殆盡。

豈料，礙於防火牆設定繁瑣，難以針對不同客戶分設客製化設定，維運人員窮於應付日趨複雜的攻擊型態，再加上防火牆存在狀態表(State Table)的致命罩門，一旦Session胃納耗盡，瞬間就會遭駭客擊垮。

借測Arbor Networks APS 驚覺流量不單純

「一次因緣際會，得知Arbor Networks的企業級DDoS防護方案Pravail APS(以下簡稱『APS』)，於是要求借測，」魏榮村說。未使用Arbor之前，魏榮村一直認爲Arbor是DDoS防禦的第一國際知名品牌，以往被認爲是大型電信才有能力部署的設備，且需要深厚專業知識，才有能力操作與設定。

然而APS到位的第一天，只是單純的啓用了在旁監看流量的Inactive模式，透過非常簡單的視覺介面，暉捷科技的網管人員赫然發現一些前所未見的惡意流量：旗下某客戶，正遭遇5Gbps DDoS流量攻擊，經由國際雲端清洗後只剩1%(也就是5Mbps流量)，按理這5Mbps應乾淨無虞，但透過APS檢測後，網管人員發現這些「洗淨」流量中高達80%比重(4Mbps)未被清洗乾淨，這些竟屬於反射放大攻擊，過去在沒有APS部屬前，以爲是主機負荷過重，所以彈性增加虛擬主機應付，以緩解主機負荷，雖然還未造致命險境，但已影響服務品質。

更甚者，平日未被大流量攻擊時的正常流量(1Mbps)，被APS檢測出1～3%流量(10K～30KBps)夾雜微量DDoS測試封包，有不明人士不斷探測該客戶的網路及系統弱點。很快的，魏榮村便決定改採兼具監看與阻擋功能的active模式，一旦觀察到惡意流量可即時擋下，又不影響客戶正常服務運行，可見APS誤判率極低，又能確實能夠有效抵禦DDoS。

▲Arbor Networks臺灣區總經理金大剛(左)與暉捷科技總經理魏榮村。

雖然這些測試封包流量微乎其微，但經過APS精準判斷及阻擋過濾後，該轄下客戶經常被攻擊的生態改變了：延長大幅降低被攻擊頻率！藉助APS掌握攻擊前兆，並加以攔阻，不僅有助保護暉捷基礎設施，亦可對客戶提供更強而有力的加值服務，連帶提高主客雙方的黏著度與信賴感，這是APS除了功能之外的另一個無形效益。

僅靠雲端自來水廠清洗 絕非抵禦DDoS良策

在經過這次的實測之後，Arbor臺灣區總經理金大剛深覺若將雲端清洗中心比喻爲自來水廠，在源頭濾除99%雜質後，算是責任已了，然而剩餘1%流量，裡頭仍可能包含濾過性病毒、細菌、雜質等有害物質，一般人敢生飲嗎？只有裝設濾水器嚴加過濾，才能確保水質乾淨無虞。

一般用戶誤以爲單憑雲端清洗即能完全防堵DDoS，顯然值得商榷，正確來說，雲端清洗加上過濾防護設備，方能符合Garner所倡導的Multi-Layer DDoS Protection必要機制，缺一不可。

尤其是在不一定會遇到DDoS洪水攻擊的前提下，在地端(on-premises DDoS appliances)專業的時時監控阻擋DDoS設備是Must-to-Have的必要部屬，雲端清洗服務(mitigation services)反倒是Nice-to-have，除非用戶已是DDoS洪水攻擊的常客，才有必要求助雲端自來水廠進行協防。

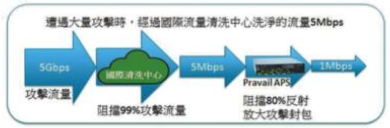
「防禦設備的重要性，遠勝流量清洗中心！」金大剛補充，經過使用Arbor產品，才發現其操作與設定門檻遠較預期低，APS具備學習能力，會依據網站或網頁對內對外的實際傳輸流量，自動產生建議參數值，方便用戶將對外服務類型按IP區段隔開，設定爲一個個保護群組，再根據參數設置不同的智慧防禦層級。

反觀其餘宣稱具DDoS防護效果的設備，皆不會給予建議值，用戶僅能根據平均值採取一視同仁設定，意即不管用戶別、服務別通通設置一致防禦層級，防護效果高下立判。

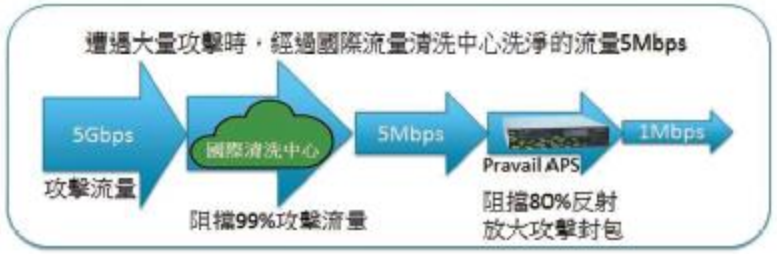
從部署順序來看，第一步是搭配連外電路頻寬部署相對throughput的APS設備，阻擋目前針對有狀態表設備的狀態耗盡攻擊(State Exhaustion Attack)及應用層攻擊(Application Attack)；流量清洗中心則是在攻擊流量大(Volumetric Attack)時的第二道防線。

金大剛指出，APS可依預先設定的水位，在瀕臨聯外線路頻寬接近滿載的臨界點前夕(目前最大可到10G)，即可向Arbor Cloud(Arbor自建的雲端清洗中心)自動發出求救信號(Cloud Signal)，由此雲端機制協助清洗流量，再回傳乾淨流量。

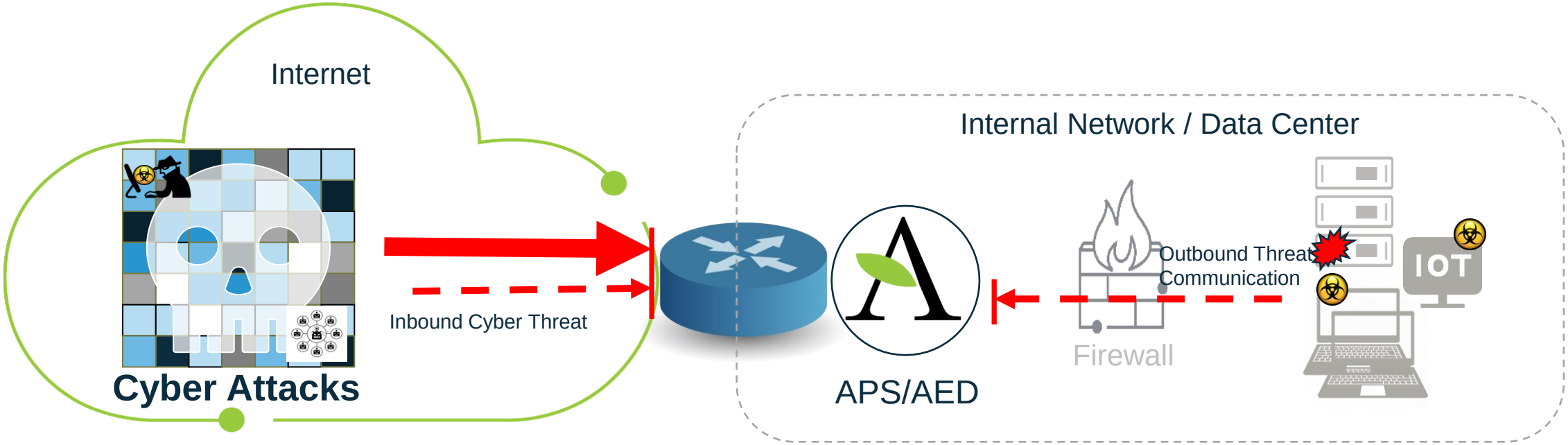
但在此同時，本地端APS設備仍持續阻擋惡意攻擊，並無其他流量清洗中心需時5～15分鐘進行流量收斂的空窗期，再者用戶亦無需建置額外路由設備，因而降低網路規劃的複雜度，且Arbor因應最新攻擊建立特徵指紋的速度，也明顯快過其他中心，相形之下，Arbor完整的DDoS防護解決方案顯然具有相對優勢。



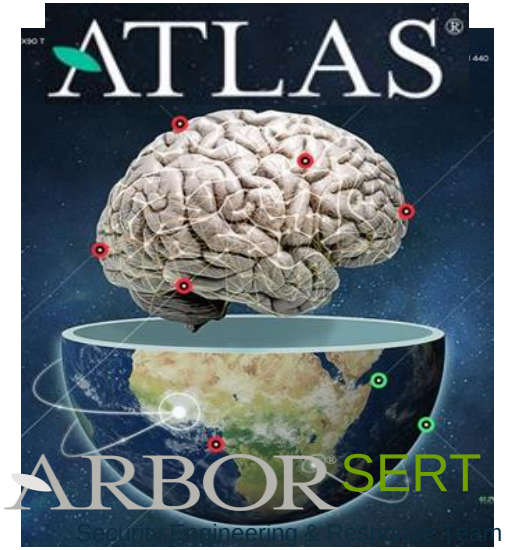
- 降低被攻擊的頻率(3天 → 5週)
- 降低被攻擊的流量(數10G → 數百Mbps)



學校不只是需要DDoS保護而已



Arbor Edge Defense(AED) = APS + ATLAS Global Threat Intelligence



學校需要主動攔截來自於外部及內部的任何形式的攻擊及威脅

AED (第一道 & 最後一道防線)

Continuous Update

- **Inbound Threats:** Detect & Stop
  - DDoS attacks.
  - Malware and other advanced cyber threats.

Outbound Threats: Identify & stop outbound threat communication

- The ability to use stateless, reputation-based, technology to match and block on IP addresses, domains and individual URLs
- Block pages that are serving up malware or used in C2 communications.

Thank You

ARBOR NETWORKS
The Security Division of NETSCOUT