

# TippingPoint UnityOne

## Co je TippingPoint a UnityOne ?

TippingPoint se po akvizici v lednu 2005 stala samostatnou divizí společnosti 3Com. UnityOne je unikátní bezpečnostní Intrusion Prevention System (IPS) produkt, jež je schopný blokovat narušení podnikové sítě a chránit jednotlivé části podnikové infrastruktury.

## K čemu je IPS ?

UnityOne je v současné době nejlepší a nejvýkonnější IPS produkt na trhu, o čemž svědčí nespočet ocenění z roku 2004 a 2005. Příkladem mohou být ocenění Gold Award od NSS Group, nebo Best Security Solution 2005 od SC Magazínu.

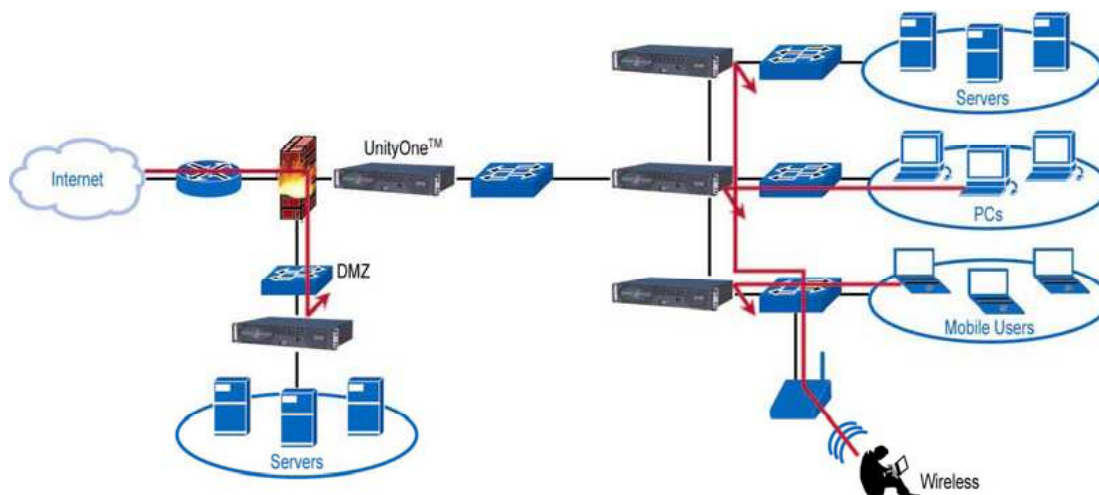
IPS systém se instaluje In-Line do datové cesty, aby odfiltroval škodlivý provoz z datové linky, kterou chceme chránit. UnityOne odstraní z datového toku například všechny součásti probíhajícího DoS (Denial Of Service) útoku, aniž by byla jakkoliv ovlivněna probíhající datová komunikace.

POZOR, zde je významný rozdíl od Intrusion Detection Systémů IDS, které pouze nebezpečný provoz detekují, ale neodstraňují jej z datového toku.

UnityOne provádí kompletní Layer7 inspekci paketů a čistí Inter/intranetový provoz od virů, červů, červů zanesených na mobilních přístrojích, trojských koňů, smíšených útoků, DoS, DdoS, zadních vrátěk či zamezuje kradení pásma škodlivými aplikacemi. UnityOne chrání síťovou infrastrukturu blokováním útoků proti routerům, přepínačům, DNS a dalším.

UnityOne IPS s unikátním paralelním zpracováním filtrů disponuje vynikajícími výkonovými parametry s minimálním zpožděním, které umožňuje in-line nasazení. Díky tomu je možné jej použít nejen v perimetru sítě, ale je vhodný také k ochraně serverů a síťových zdrojů na výkonných linkách, k oddělení skupin uživatelů, WAN, vzdálených uživatelů nebo bezdrátových klientů.

Schéma znázorňuje příklad nasazení UnityOne v podnikovém prostředí k ochraně perimetru, DMZ, serverů, stanic a mobilních klientů.



## Hlavní funkce

UnityOne kromě IPS funkcí slouží k ochraně:

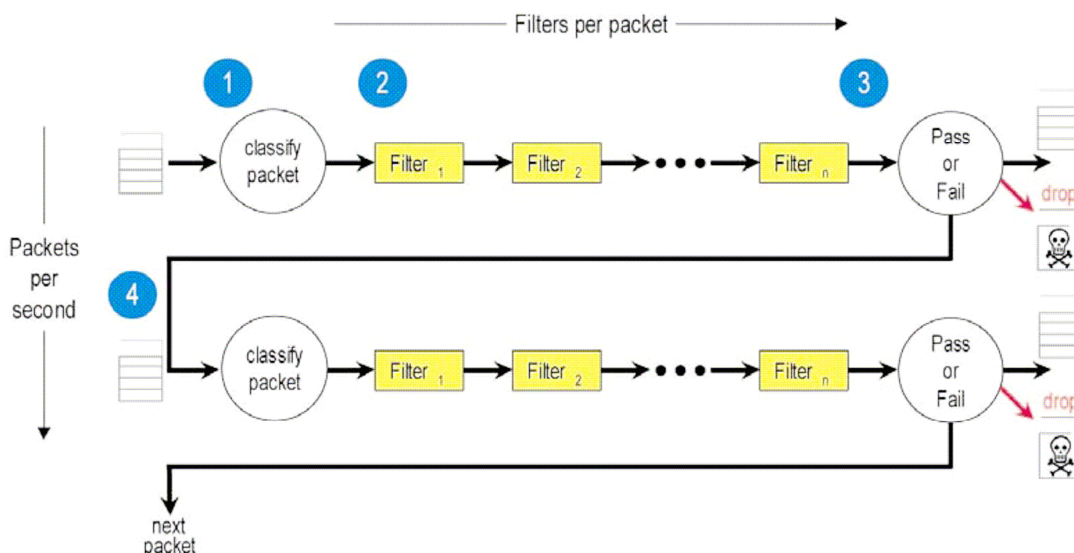
- Aplikací a OS
- Infrastruktury ochranou síťových zdrojů
- Výkonu tvarováním dat a potlačením škodlivých dat

## Výkon

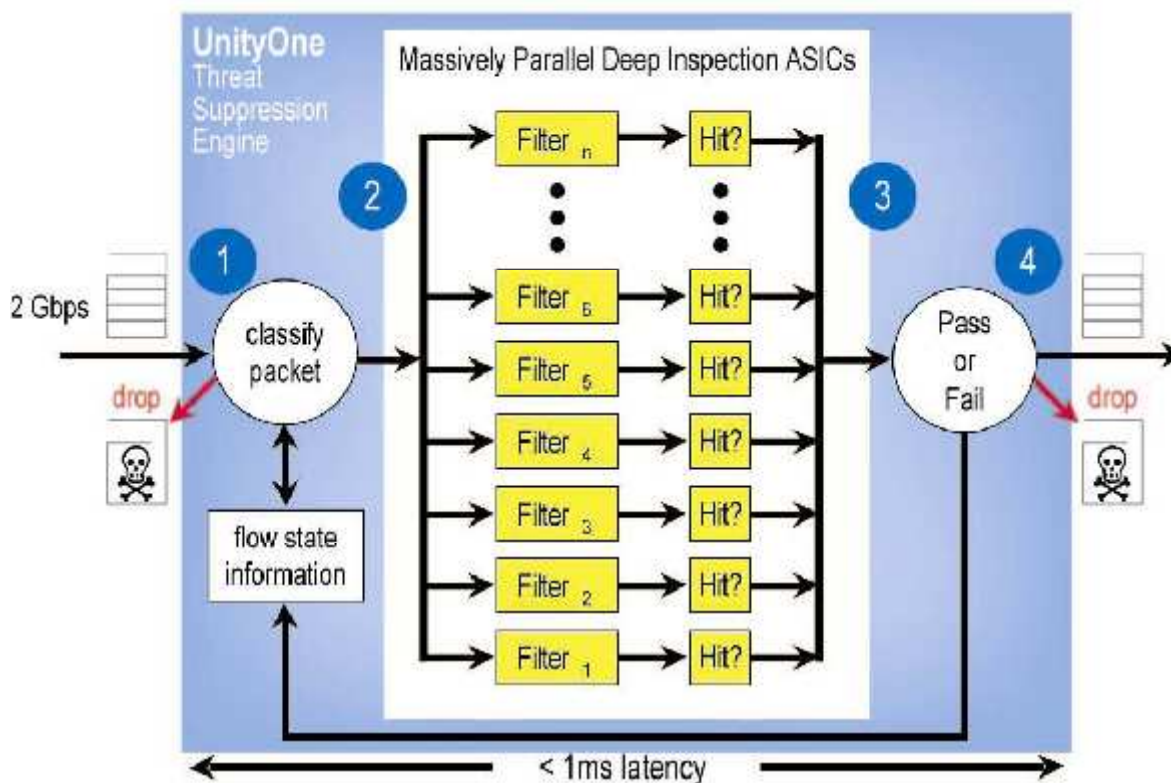
Jednou z klíčových a oceňovaných vlastností jsou masivně paralelní kontrolní procesy, kdy je tok dat paralelně konfrontován s nahanými filtry. Tento proces má díky programovatelným ASIC obvodům minimální zpoždění a odstranění škodlivých toků nemá vliv na tok dat aplikací (výsledky viz nezávislé testy latence společnosti Tolly Group). Jednotlivé produkty umožňují škálovat průchodnost od 50Mbps do 5Gbps, podle typu použití v perimetru sítě nebo na výkonných serverových linkách.

## Srovnání tradiční metody softwarového filtru s řešením UnityOne

Softwarové řešení zpracovává pakety sériově a nemůže efektivně násobit počet filtrů bez snížení výkonnosti. (1) Packet vstupuje do systému a je klasifikován, (2) je podrobován kontrole na každý platný filtr, (3) v případě shody jsou pakety zahazeny a (4) další paket je zpracován.



UnityOne Threat Suppression Engine pracuje na 2 Gbps se zpožděním pod milisekundu. (1) Paket je klasifikován, (2) všechny platné filtry jsou zpracovány současně v paralelním poli, zatímco další paket je klasifikován, (3) výsledek srovnání paralelního porovnání filtrů určí, zda paket (4) projde, nebo je zahazen. Případné zahazení je včetně všech následujících paketů patřících k stejnému toku.



## Management

UnityOne je z hlediska použití v síti transparentní, z pohledu datového toku nemá MAC ani IP adresu, takže nemá vliv ani na redundantní protokoly použité v síti, jako je například VRRP, OSPF, atd. UnityOne má management adresu oddělenou od datového toku, která se používá pro vzdálenou správu systému, logování a pro nahrání nových filtrů.

## Klíčové funkce a parametry UnityOne

Výkon	škálovatelná průchodnost od 50Mbps do 5Gbps, s latencí <215µsec, přes 2 miliony současných session TCP, UDP/ICMP, přes 250 tisíc spojení za vteřinu
Ochrana serverů a klientů	zabrání útokům proti zranitelným aplikacím a operačním systémům, umožňuje nahradit časově náročné upgrady aplikací "síťové záplaty", viz <a href="http://www.tippingpoint.com/technology_virtualpatch.html">http://www.tippingpoint.com/technology_virtualpatch.html</a>
Ochrana síťové infrastruktury	ochrana DNS služeb, Cisco IOS routerů a přepínačů, ochrana dalších síťových prvků, ochrana proti DoS, SYN Floods, aplikace přístupových filtrů ACL
Normalizace datového provozu	zvýšení pásma a výkonu směrovačů, optimalizace výkonu a normalizace neplatných dat, řízení "nenormálního" provozu nastavením limitů, <a href="http://www.tippingpoint.com/technology_threshold.html">http://www.tippingpoint.com/technology_threshold.html</a>
Ochrana aplikací	zvýšení propustnosti a kapacity serverů, filtrování nebo nastavení limitu pro nechtěná data nebo aplikace (PeerToPeer, SpyWare, AdWare atd.), ochrana datových linek pro užitečné aplikace
Digitální vakcína	automatická celosvětová distribuce nových filtrů zajistí okamžitou ochranu sítě proti novým typům narušení. Kategorizovaný seznam posledních vakcín je dostupný na <a href="http://www.tippingpoint.com/resources_@RISK.html">http://www.tippingpoint.com/resources_@RISK.html</a>
Redundance a vysoká dostupnost	duální zdroje, manuální nebo automatický Layer2 fallback v případě interní chyby, redundance Active-Active i Active-Passive, Zero Power High availability v případě úplného výpadku napájení

## Ocenění

TippingPoint UnityOne získal celou řadu ocenění. Zahrnují například:

- **NSS Group**, Gold Award v testu IPS systémů
- **SC Magazine**, Best Security Solution roku 2005
- **Common Criteria Certification**, 4 kategorie analyzer, senzor, scanner a system
- **Information Security Magazine**, IPS produkt roku 2004
- **SANS institute**, Trusted Tool
- **Frost&Sullivan**, 2005 Infrastructure protection Company of the year
- **eWeek**, Enterprise Resource Protection Excellence Award
- **IDG**, 2004 Network Protection Product of the year
- **Tolly Group**, Up to Spec performance and security test
- **eWeek**, Labs Analyst's Choice Award

## **Produktové informace**

Produktové informace je možné najít na webu  
[http://www.tippingpoint.com/resources\\_datasheets.html](http://www.tippingpoint.com/resources_datasheets.html)

## **Produktové testy**

Produktové testy třetích stran je možné najít na webu  
[http://www.tippingpoint.com/resources\\_reports.html](http://www.tippingpoint.com/resources_reports.html)

## **Aplikační návody**

Existuje celá řada opakujících se bezpečnostních situací. Existují způsoby, jak vyzkoušeným způsobem navrhnout ochranu před typickou bezpečnostní situací. Některé aplikační návody si můžete vyžádat v 3Com, některé je možné najít je na webu, zde jsou příklady:

- Ochrana portu 80,
- Zabezpečení centra sítě,
- Ochrana univerzitního prostředí proti P2P,
- Ochrana serverové farmy,
- Ochrana VoIP provozu, <http://www.tippingpoint.com/pdf/resources/datasheets/U1006.pdf>
- Ochrana před SpyWare, <http://www.tippingpoint.com/pdf/resources/datasheets/U1017.pdf>
- Zero Power High Availability, <http://www.tippingpoint.com/pdf/resources/datasheets/U1012.pdf>
- Advanced DoS FAQ, <http://www.tippingpoint.com/pdf/resources/datasheets/U1009.pdf>