České vysoké učení technické v praze
Fakulta elektrotechnická

Bezpečnost počítačových sítí

Jan Závorka

Uvod

Vzhledem ke stále rostoucímu množství útoků na aplikace jak z vnějšku sítě (Internet), tak z jejích vnitřních sítí, tak implementace řešení, schopného tyto útoky zastavit nabývá na významu.

1. Firewall

Klasický firewall poskytuje ochranu před útoky na služby, které nejsou provozovány, příslušné porty jsou zavřeny.

Nastavení pravidel pro komunikaci přes firewall se běžně označuje termínem „bezpečnostní politika firewallu“, zkráceně „bezpečnostní politika“. Bezpečnostní politika zahrnuje nejen samotná pravidla komunikace mezi sítěmi, ale u většiny dnešních produktů také různá globální nastavení, překlady adres (NAT), instrukce pro vytváření šifrovaných spojení mezi šifrovacími branami (VPN – Virtual Private Networks), vyhledávání možných útoků a protokolových anomálií (IDS – Intrusion Detection Systems), autentizaci a někdy i autorizaci uživatelů a správu šířky přenosového pásma (bandwidth management).

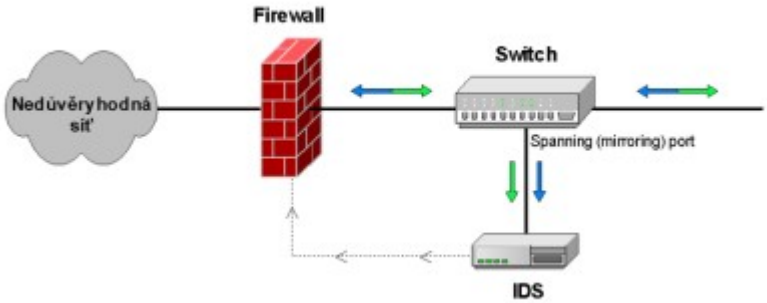
Existují však služby z venku dostupné (jako např. web, pošta aj.). Útočník tak může využít chyby v aplikaci nebo samotném operačním systému nebo serveru nabízejícího danou službu. Pro účinnou ochranu je v takovém případě nutné použít zařízení nebo aplikaci, která je schopna monitorovat provoz za otevřenými porty firewallu (IDS Intrusion Detection System), nebo lépe, která je kromě vlastního monitoringu schopna sama aktivně na případný útok reagovat (IPS Intrusion Prevention System).

Pomocí systémů detekce a prevence narušení lze vytvořit druhou obrannou linii za firewally určenou k ochraně aplikací komunikujících vně chráněné sítě.

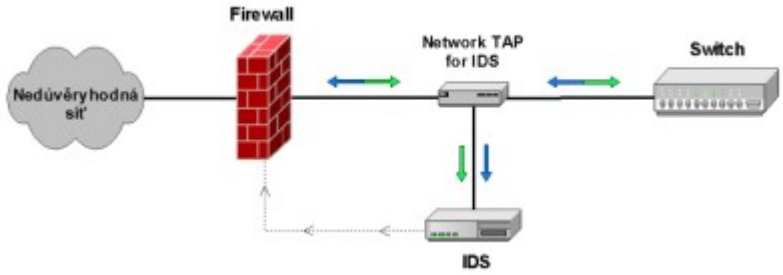
Pohled pod pokličku technologií IDS/IPS

2. IDS

sleduje datové toky a hledá v nich pokusy o útok na konkrétní aplikace. Jedná se o pasivní zařízení, pouze sleduje, nezasahuje do provozu sítě. Prostřednictvím alertů a statistik poskytuje obsluze informace o útocích. IDS sonda se nejčastěji připojuje k HUBu nebo na zrcadlový port



anebo pomocí síťového tapu



K vlastní analýze paketů používá 2 základní technologie. Zařízení a aplikace renomovaných výrobců obě kombinují.

- Signatury (unikátní sekvence znaků)
  Technika spočívá v hledání určitých znakových sekvencí v datovém toku. Vzhledem ke generování vyššího množství falešných poplachů byla technika dále zdokonalena o detekci stavu. Vyhledává se nejen znaková sekvence, ale zároveň se zjišťuje, zda-li se tato sekvence nachází ve správné části datového toku. Pro správnou funkci této metody musí být zařízení vybaveno databází signatur jednotlivých útoků. Zařízení jsou schopna si tuto databázi sama automaticky průběžně doplňovat.
- Dekódování protokolů
  Systém dekóduje jednotlivé protokoly a v takto dekódovaném provozu vyhledává obecné zranitelnosti jako je kupříkladu přetečení vyrovnávací paměti.

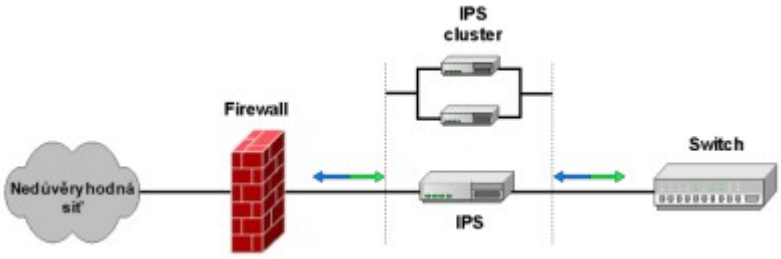
3. IPS

Systém prevence průniků (IPS - intrusion-prevention system) je moderní součástí celkové strategie ochran počítačové sítě. Jedná se o podstatné rozšíření ochrany poskytované Firewallem. Běžný SPI firewall je totiž schopný vidět v paketu pouze do úrovně zdrojových a cílových portů. Pro firewall korektní provoz na TCP portu 80 tak klidně může obsahovat škodlivý kód, který není firewall schopen detekovat a blokovat, protože je přenášen ve vrstvě, do které firewall "nevidí". IPS zkoumá veškerý provoz až do sedmé vrstvy OSI protokolu, který prošel firewallem a případně i vnitřními segmenty sítě. Provede "odfiltrování" škodlivého obsahu na základě porovnání se známými obrazci z databáze, může využívat i heuristickou analýzu a uživatelsky definované filtry.

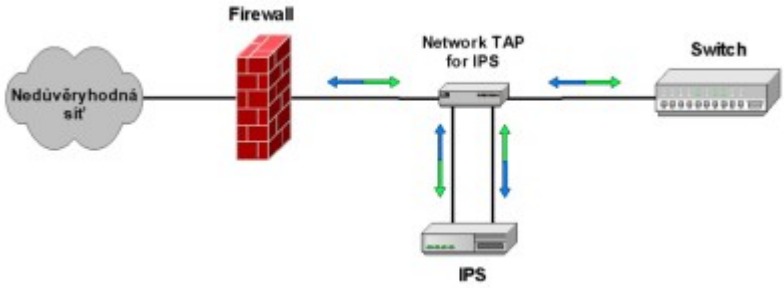
Zde je významný rozdíl oproti IDS systémům (Intrusion Detection Systém), které nebezpečný provoz pouze DETEKUJÍ, ale neodstraní jej z datového toku. IPS provádí kompletní inspekci paketů až po 7. (aplikační) vrstvu a čistí internetový nebo intranetový provoz od virů, červů, trojských koní, chrání vnitřní síť před útoky typu DoS (Denial of Service), DDoS (Distributed Denial of Service), před útoky využívajícími otevřených zadních vrátek, škodlivými aplikacemi kradoucími pásmo, i před různými smíšenými útoky. IPS lze nasadit

jako univerzální síťovou záplatu, která umožní oddálit nebo úplně nahradit instalaci záplat na jednotlivé stanice a servery s náročným testováním kompatibility aplikací, protože IPS probíhající útok na servery či stanice z datového toku odstraní. IPS chrání síťovou infrastrukturu blokováním útoků proti routerům, přepínačům, DNS serverům a dalším.

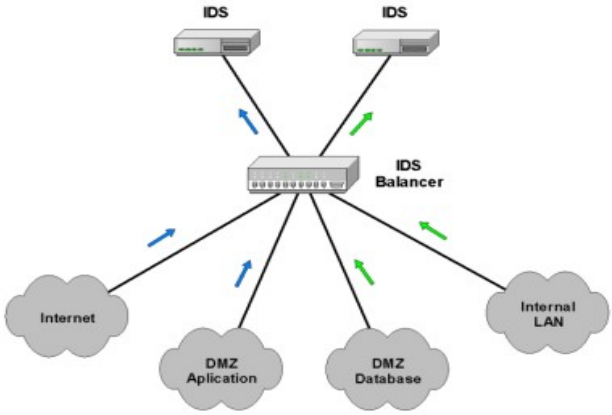
nejen detekuje pokusy o útok jako IDS, ale zároveň je schopno dle nastavené konfigurace aktivně reagovat, tzn. útoku zabránit. Jelikož IPS sonda musí být schopna v případě potřeby modifikovat datový tok, instaluje se přímo mezi rozpojenou monitorovanou datovou linku.



Aby byla možnost komunikace i v případě neprůchodnosti IPS sondy, např. vlivem poruchy, volí se zapojení se síťovým tapem.



Pomocí IDS balanceru je možno agregovat více vstupů do jediného datového toku a ten poté předat jedné IDS sondě.



Výhoda takové topologie spočívá především v možnosti ušetřit náklady spojené s nasazením více sond v prostředí, kde zátěž jednotlivých linek není na hranici propustnosti sondy. V případě, že použijeme dva výstupy a následně dvě sondy, lze využít výhod load balancingu a vysoké dostupnosti.

Integrovaná řešení

Existují řešení začleňující modul IDS do vlastního firewallu, jako například Checkpoint SmartDefense ve FireWallu-1, nebo modul Deep Packet Inspection ve firewallech společnosti Netscreen. U nasazení, kde je potřeba zvýšení úrovně zabezpečení , je nutné provozovat firewall a IDS/IPS odděleně. Zabrání se tak možnosti selhání jak firewallu, tak IDS v případě kompromitace jednoho systému.

Další možností kooperace firewallu a IDS je schopnost IDS, přimět firewall ke změně chování (politiky). Takto kooperují systémy podporující standard OPSEC. Funkcionalita tohoto řešení však plně nenahrazuje systém prevence narušení, protože IPS je schopen spojení zastavit ještě před jeho navázáním.

Lidský faktor

Je třeba zdůraznit, že plné využití vlastností systémů detekce a prevence narušení jde ruku v ruce s jejich vhodným začlením do síťového prostředí a správnou konfigurací.

4. NetworkLogin 802.1x

Zabezpečení počítačové sítě pomocí funkce NetworkLogin 802.1x umožňuje aktivnímu prvku bezpečně ověřit uživatele na základě uživatelského jména a hesla a teprve po ověření jej připustit ke zdrojům sítě. Aktivním prvkem může být v tomto případě přepínač, přístupový server, bezdrátový přístupový bod (AP). Ověřovací autoritou není aktivní prvek sám, ale centrální databáze uživatelů, se kterou jako její klient komunikuje. Tato databáze se nazývá RADIUS (Remote Authentication Dial In User Service - RFC 2865). RADIUS server je možné provozovat jako službu integrovanou v Microsoft ActiveDirectory. Celý proces ověření probíhá tak, že stanice (v terminologii 802.1x Suplicant) se připojí k portu zabezpečenému 802.1x. Svoji existenci přepínači dá najevo libovolným paketem, například požadavkem o přidělení IP adresy. Přepínač však přijatý DHCP požadavek nepřeposílá dál, ale obratem posílá žádost o identifikaci zpět na stanici. Stanice odpovídá svým uživatelským jménem a heslem. Přepínač přijaté informace zašifruje do paketu a pošle na ověřovací autoritu. RADIUS server provede vyhodnocení přijatých informací a zpět přepínači odešle potvrzení či odmítnutí uživatele. Přepínač na základě této informace vpustí či odmítne stanici přístup do takto zabezpečené sítě.

Metody ověřování

Stanice může být ověřena na základě uživatelského jména a hesla nebo digitálního certifikátu. Ověřování pomocí digitálního certifikátu vyžaduje, aby v síti byla instalována Certifikační autorita a stanice měly přidělené digitální certifikáty.

Network Login pracovní módy

Network Login blokován
- Klienti bez bezpečnostního mechanismu budou mít přístup do sítě

Standardní Network Login
- Bude vyžadována autentizace neautorizovaných klientských portů
- Port přepínače, který byl již autentizován, bude otevřen - Tento pracovní mód

umožňuje přístup neautorizovaných stanic do sítě například použitím opakovače nebo přepínače, za nímž bude jediná ověřená stanice. Z hlediska úrovně poskytované bezpečnosti je nutné se tomuto módu pokud možno vyhnout.

Zabezpečený mód

- MAC adresa je zaznamenána oproti portu autorizace bude platná pouze proti MAC adrese která ověření provedla.
- Bude předáván pouze provoz do a z této MAC
- Druhá a případné další MAC adresy viděné na portu budou blokovány
- Tento mód je vhodný pro omezení množství připojených stanic na koncových přepínačích na jednu per port.

Má to však nevýhodu, tento mód nelze použít souběžně s hardware IP telefonie (VoIP telefony s integrovaným dvouportovým bridge) či virtualizací systému nástroji typu VMWare či Virtual PC v bridge modu. Virtualizační nástroje mohou pracovat v NAT režimu na ověřované stanici bez omezení.

Vícenásobně zabezpečený mód

- " MAC adresa stanice je zaznamenána oproti portu, na kterém provedla úspěšné 802.1x ověření a dále bude předáván pouze provoz do a z této MAC adresy
- Na tom samém portu se mohou autentizovat další uživatelé pro získání přístupu
- Stanice, jejíž MAC adresa neprovedla úspěšné ověření, bude vyřazena z provozu, aniž to ovlivní činnost na portu již ověřených stanic
- Až 1024 uživatelů na jednom portu přepínače 3Com Switch 7700 (256 na přepínači 3Com Switch 5500 a 3Com Switch 4500)

RADA

Radius Authenticated Device Access - modifikace technologie Network Login, která umožní přihlášení do sítě na všechna zařízení, bez ohledu na klienta, tedy například i síťové tiskárny, IP telefony, bezdrátové přístupové body, terminály a podobně. Toto rozšíření umožní namísto ověření 802.1x použití MAC adresy konzového zařízení pro potřeby ověření v centrální databázi RADIUS serveru. RADA navíc umožňuje definovat řízený přístup k síti pro dočasné uživatele, které začlení do definované hostitelské oblasti, například s přístupem pouze do Internetu. RADA tak používá k ověření fyzickou adresu stanice, ale lze ji kombinovat i s ověřením přes 802.1x. Síť potom rozlišuje, zda je připojeno povolené zařízení nebo neznámý počítač, případně v kombinaci s přihlášením rozlišuje i práva uživatele. Tyto způsoby ověření podporují i automatické zařazení uživatele ke skupině (AutoVLAN) nebo automatické nastavení kvality služby (AutoQoS). V této souvislosti je třeba zmínit, že existují postupy, jak měnit fyzickou MAC adresu síťových rozhraní, nicméně tato procedura není obecně známá běžným uživatelům výpočetní techniky. Doporučeno je omezit použití RADA technologie pro ověřování pouze a právě jen zařízení, v nichž není podpora 802.1x implementována a takto ověřená zařízení zařazovat do virtuálních sítí určených pro specifický provoz (například VLAN pro síťové tiskárny a scannery či VLAN pro VoIP).

5. DoS a DDoS útoky a ochrana proti nim

Denial of Service (česky *odmítnutí služby*) nebo též **Distributed Denial of Service** (česky *distribuované odmítnutí služby*) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele.

Co znamená útok Denial of Service?

Denial of Service (DoS) útoky jsou síťové útoky, které brání přístupu ke službám. DoS útoky blokují služby sítě zaplavováním spojení, zhroucením serverů nebo programů běžících na serverech, vyčerpáváním zdrojů na serveru nebo jinak brání legitimním klientům v přístupu ke službám sítě.
Denial of Service (DoS) útoky jsou síťové útoky, které brání přístupu ke službám. DoS útoky blokují služby sítě zaplavováním spojení, zhroucením serverů nebo programů běžících na serverech, vyčerpáváním zdrojů na serveru nebo jinak brání legitimním klientům v přístupu ke službám sítě.
DoS útoky mohou mít celou škálu podob, od útoku jednoho paketu (single packet atack), který způsobí zhroucení serveru, až po koordinované záplavy paketů od mnoha hosts. Při útoku jednoho paketu je poslán do sítě pečlivě přizpůsobený paket, který využívá známé zranitelnosti operačního systému nebo aplikace a zablokuje server a/nebo některé služby jím poskytované. Slammer worm využívá jedné takové zranitelnosti.
Při záplavovém útoku jsou zdroje na serveru nebo na síti narušeny nebo vyčerpány záplavou paketů. Po napadení jednoho místa může být záplava celkem snadno identifikována a izolována. Mnohem sofistikovanější přístup, zvaný Distributed DoS (DDoS) útok, je nástroj pro mnoho záplavových útoků. Při DDoS útoku používá útočník k zasažení cíle množství počítačů. Některé útoky mají jednoduchý plán, jako třeba poslání nekonečného proudu dat k zaplavení síťových spojení na serveru. Jiné útoky, jako třeba SYN záplavy, používají pečlivě upravené pakety k vyčerpání kritických zdrojů za účelem zabránit legitimním klientům v připojení k serveru.
Bez ohledu na druh, k DDoS útoku se používá určitý počet přístrojů s koordinovaným chováním. Tyto přístroje, známé jako zombies, byly předtím kompromitovány a jsou pod kontrolou útočníků. Posíláním příkazů těmto zombies přes skryté komunikační kanály mohou hackeři inscenovat rozsáhlé koordinované útoky. Protože útok pochází od velkého množství počítačů rozmístěných po celé síti, jednoduchá identifikace a izolace není možná. V mnoha případech je extrémně obtížné oddělit legitimní provoz od útočného. S nárůstem počtu počítačů, které získávají širokopásmový přístup z domova, narůstá i množství potenciálních zombies. Experti odhadují, že 1/3 domácích uživatelů Internetu byla kompromitována. Požadavky na sofistikovanost a zábrany proti šíření těchto DDoS útoků byly výrazně sníženy díky dostupnosti sad nástrojů (např. Tribe Flood Network a Stacheldracht), které jsou volně dostupné na Internetu.

TippingPoint řešení

Jako odpověď na rozvoj DoS a DDoS útoků vyvinul TippingPoint arzenál ochranných mechanismů korespondujících s metodami, které využívají útočníci. Systém prevence průniků TippingPoint (Intrusion Prevention System - IPS) pracuje in-line a chrání síť a k ní připojené hosts tak, že prověřuje každý bit procházejícího provozu a odfiltrovává nežádoucí provoz.
TippingPoint primárně poskytuje dva druhy ochrany: Standardní ochranu před DoS a pokročilou ochranu před DDoS. Standardní DoS ochrana poskytuje základní úroveň ochrany před zranitelnostmi, nástroji útoků a anomáliemi provozu. Pokročilá DDoS ochrana chrání před útoky typu SYN floods, established connection flood a connections per second flood.
Všechny IPS produkty TippingPoint poskytují standardní DoS ochranu:

- **Vulnerability Protection** (ochrana před zranitelnostmi) - chrání před DoS útoky, které způsobují zhroucení serverů využitím známých zranitelností.
- **Zombie Recruitment Protection** (ochrana před náborem zombies) - chrání před náborem zombies ze systémů pomocí programů Trojan.
- **Attack Tool Protection** (ochrana před nástroji útoků) - blokuje přeměněné kanály použité dobře známými programy pro DDoS útoky včetně TFN, Loki a Stacheldraht.
- **Bandwith Protection** (ochrana šíře pásma) - chrání před záplavami paketů jako ICMP, TCP nebo UDP, které mohou spotřebovávat šíři pásma sítě nebo zdroje serveru a tím způsobovat zahazování legitimních pakteů. Tyto filtry usměrňují a přiškrcují provoz, když se dostane nad nastavené procento.

Pokročilá DDoS ochrana poskytuje navíc ochranu před následujícími útoky:

- **SYN Proxy** - útočník zaplaví server zlovolnými požadavky na spojení (TCP SYNs) s falešnými zdrojovými IP adresami, čímž zabrání legitimním klientům v připojení k serveru.
- **Connection per Second** (CPS) Flood (záplava spojení za sekundu) - útočník využívá armádu zombies k opakovaným požadavkům na zdroje, jako třeba webové stránky, od serveru. Výsledná zátěž zpomalí server nebo ho znepřístupní.
- **Established Connection Flood** (záplava založených spojení) - útočník využívá armádu zombies k založení rozsáhlého počtu - potenciálně miliónů - zlovolných TCP spojení se serverem, čímž serveru zabrání v přijímání nových požadavků od legitimních klientů.

Standardní a pokročilá DoS a DDoS ochrana pracují společně k zastavení chirurgické a brutální síly DoS útoků a ochraně před náborem nových zombies.

Sedm běžných metod DoS útoků

Hackeři mají celý arzenál metod k provádění Denial of Service (DoS) útoků. Následujících sedm oddílů ukazuje rozsah problémů, kterým musí čelit organizace při boji proti DoS hrozbě.
TippingPoint poskytuje řešení v boji proti těmto běžným metodám DDoS útoků:

- **Vulnerabilities** (zranitelnosti)
- **Zombie Recruitment** (nábor zombies)
- **Attack Tools** (nástroje útoku)
- **Bandwith attacks** (útoky na šíři pásma)
- **SYN Floods** (záplavy SYN)
- **Established Connection Floods** (záplavy založených spojení)
- **Connections-Per-Second Floods** (záplavy spojení za sekundu)

Metoda 1 - Vulnerabilities (zranitelnosti)

Útočníci se mohou pokusit způsobit zhroucení služeb nebo základního operačního systému přímo prostřednictvím sítě. Tyto útoky blokují poskytování služeb pomocí nárazových záplav a využití různých "zadních vrátek", která existují u nechráněných serverů. Útoky na zranitelnosti nevyžadují ke své realizaci žádné rozsáhlé zdroje nebo šíři pásma; útočníkům stačí pouze znalost zranitelností, aby je mohli využít a způsobit rozsáhlé poškození. Jakmile útočník získá kontrolu nad zranitelnou službou, aplikací nebo operačním systémem, zneužije toho k zablokování systému a konečnému vnitřnímu zhroucení celé sítě.

TippingPoint řešení pro zranitelnosti

TippingPoint poskytuje výkonný nástroj, který detekuje a blokuje pokusy o využití zranitelností pro veškerý příchozí i odchozí provoz. Bezpečnostní tým TippingPoint průběžně vyvíjí filtry proti útokům určené pro odhalené zranitelnosti v síťových službách a operačních systémech a začleňuje tyto filtry do digitálních vakcín. Digitální vakcíny jsou dodávány zákazníkům každý týden nebo okamžitě při objevení kritické zranitlenosti. Mohou být umísťovány automaticky, bez zásahu uživatele, aby poskytovaly automatickou ochranu.

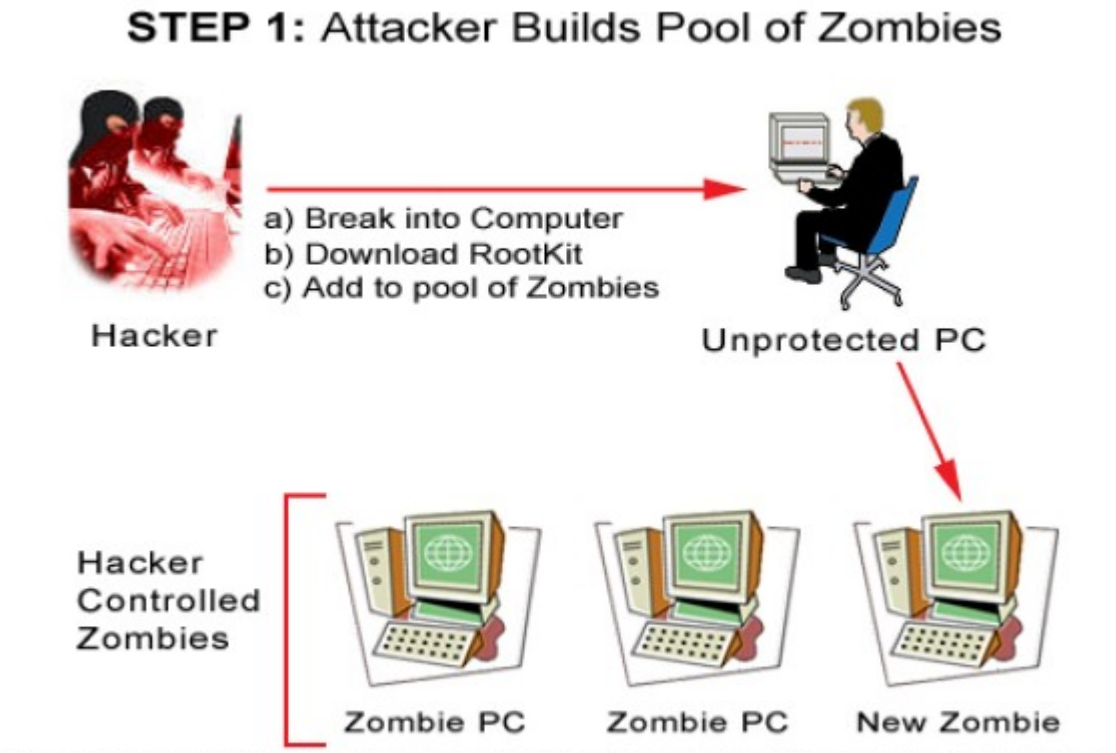
K provedení útoku využitím velkého počtu hosts, kteří útočí současně, útočníci infikují hosts zombií nebo agentským programem, který připojuje předdefinovaného master host. Jakmile je připojen, útočník může posílat příkazy napříč celou sítí zombie.
TippingPoint chrání proti zombie útokům detekováním a blokováním virů používaných k zavedení zombie agenta.

Metoda 2 - Zombie Recruitment (nábor zombií)

Ty samé zranitelnosti použité ke shození serveru umožňují hackerům transformovat zranitelné počítače na zombies. Jakmile hacker využije zranitelnost k získání kontroly nad systémem, umístí do systému "zadní vrátka" pro pozdější využití při provedení DDoS útoku. Trojan nebo podobná infekce umožní path do systému. Jakmile má útočník path, může na dálku kontrolovat síť, přeměnit server na zombie čekající na příkaz k útoku. Pomocí takových zombies mohou útočníci posílat velké množství DoS a DDoS útoků a zůstat přitom v anonymitě.
Pro nábor zombies mohou být využity i viry. Například virus MyDoom byl přímo vyvinut aby přeměňoval počítače na zombies, které pak napadly SCO a Microsoft v předem určeném čase naprogramovaném v tomto viru. Další viry instalují "zadní vrátka", která umožňují hackerům spuštění koordinovaných útoků s narůstající hustotou napříč sítěmi na celém světě.

Následující obrázky detailně ukazují, jak útočníci zahajují útoky na síť.

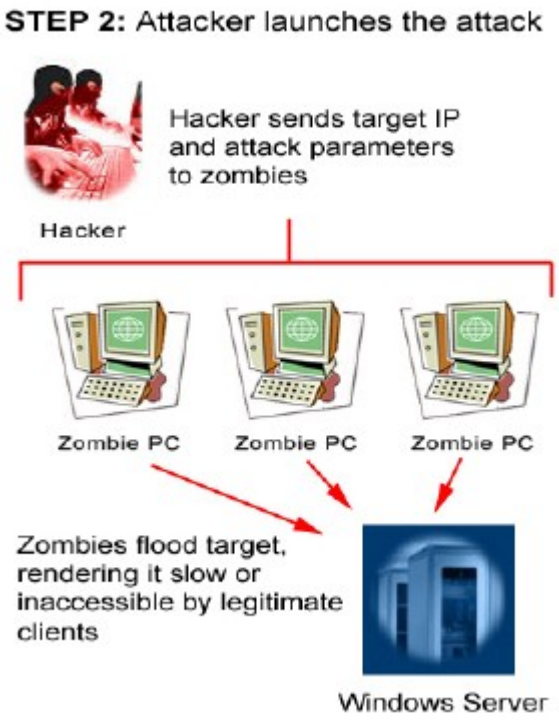
KROK 1: Útočník vytváří skupinu zombies



The attacker builds a pool of zombies by compromising unprotected computers.

Útočník vybuduje skupinu zombies kompromitováním nechráněných počítačů

KROK 2: Útočník zahajuje útok



Útočník zahajuje útok proti serveru/síti použitím zombie počítačů. Útok ochromuje výkon a blokuje legitimní provoz na síti.

TippingPoint řešení náboru zombies

Kromě dříve uvedené ochrany před zranitelnostmi, obsahuje TippingPoint i filtry, které detekují a blokují viry. Kombinací účinků filtrů proti virům a zranitelnostem je dosaženo virtuální nemožnosti náboru nových zombies hackery.

Metoda 3 - Attack Tools (nástroje útoku)

Pomocí náboru zombies používají hackeři přeměněné komunikační kanály ke kontrole a kontaktování armády zombies. Mohou si vybrat ze stovek programů pro tvorbu "zadních vrátek" a zákaznických nástrojů, které jsou k dispozici na internetu. Díky těmto nástrojům a programům pronikají armády zombies do sítě a získávají nad ní kontrolu, aby mohly později zaútočit zevnitř. Jakmile má hacker systém zombies, může použít další nástroje k současnému poslání jednoho příkazu všem zombiím. V některých případech jsou příkazy přenášeny v ICMP nebo UDP paketech. které mohou obcházet firewally. V jiných případech zombie "volá domů" vytvořením TCP spojení k masterovi. Jakmile je toto spojení vytvořeno, master může kontrolovat tuto zombii.

Nástroje používané k útoku a kontrole nad systémy zahrnují:
- **Tribe Flood Network** (TFN) - zaměřuje se na Smurf, UDP, SYN a ICMP echo request záplavy
- **Tribe Flood Network 2000** (TFN2K) - aktualizovaná verze TFN
- **Trinoo** - zaměřuje se na UDP záplavy. Posílá UDP pakety na náhodně zvolené cílové porty. Velikost je konfigurovatelná.
- **Stacheldraht** - softwarový nástroj, který je zaměřen na TCP, ACK, TCP NULL, HAVOC, DNS záplavy a záplavy TCP pakteů s náhodným záhlavím. DDoS nástroje se zdokonalují jak co se týče utajení využívaných kanálů, tak i technik DDoS záplav. Nové nástroje využívají libovolná čísla portů nebo pracují napříč IRC. Dále promyšlenější nástroje inteligentně maskují záplavové pakety jako legitimní požadavky na provoz a/nebo uvádějí vysoký stupeň náhodnosti. Pro zařízení filtrující na portech narůstá díky těmto vylepšením obtížnost na oddělování útočných paketů od legitimního provozu.

TippingPoint řešení pro DDoS nástroje

TippingPoint nabízí stovky filtrů, které přesně detekují a blokují přeměněné komunikační kanály, narušují příkazy a kontrolu nad sítí od DDoS armády hackera. Kombinací ochrany před viry a zranitelnostmi TippingPoint zabraňuje náboru nových zombies, brání stávajícím zombies v komunikaci a poskytuje administrátorovi detailní informace potřebné k vyčištění napadeného systému.

Metoda 4 - Bandwith Attacks (útoky na šíři pásma)

DDoS útok může být detekován už při zahájení jako signifikantní změna ve statistickém složení provozu na síti. Například, typická síť může sestávat z 80-ti procent TCP a 20-ti procent směsi UDP a ICMP. Změna ve statistickém složení může být signálem nového útoku. Kupříkladu červ Slammer způsobuje nárůst UDP paketů, zatímco červ Welchi vytváří záplavu ICMP paketů. Jakýkoliv takový nárůst může být DDoS útokem nebo takzvaným zero-day útokem - to je útok, který využívá dosud neodkryté zranitelnosti.

TippingPoint řešení útoků na šíři pásma

TippingPoint IPS je vybaven filtry statistických anomálií, které detekují záplavy paketů a usměrňují rozsah, aby zmírnily jejich účinky. TippingPoint poskytuje také filtry pro prahové hodnoty provozu protokolů i aplikací. Filtry prahových hodnot provozu protokolů mohou být vytvořeny pro TCP, UDP, ICMP a další IP protokoly. Filtry prahových hodnot provozu aplikací monitorují provoz na určitých TCP a UDP portech. Oba typy filtrů statistických anomálií vytvářejí základní linii normální úrovně jednoho typu provozu a upozorňují na nárůst tohoto typu provozu nad uživatelem definovanou úroveň. Například můžete vytvořit filtr prahových hodnot protokolu, který vytvoří základní linii normální úrovně ICMP provozu a pošle upozornění, když úroveň provozu překročí 300% normálu.

Pro poskytování lepší ochrany sítě má TippingPoint začleněné pokročilé monitorování charakteru provozu a filtry pro sledování a reagování na možné anomálie provozu. Takové náhlé změny v provozu mohou znamenat útok. S těmito pokročilými vlastnostmi poskytuje UnityOne nejlepší ochranu majetku organizací.

Navíc kromě upozornění, dokáže TippingPoint ochránit monitorovaný provoz před překročením nebo větším spotřebováváním šíře pásma než je současná úroveň. Například když ICMP provoz překročí 500% normálu, může být omezen jeho rozsah tak, aby neužíval více než 3 Mbps. Tato výkonná schopnost kontroluje nadměrné spotřebovávání šíře pásma aplikacemi, které nejsou kritického významu, a zajišťuje dostupnost šíře pásma pro aplikace s kritickým významem. Agresivně šířený provoz produkovaný současnými červy má za následek DoS útoky proti směrovačům, firewallům a ostatním částem infrastruktury sítě. Limitování tohoto provozu na omezenou šíři pásma udrží síť v provozu a potlačí útok.
Filtry prahových hodnot provozu jsou spouštěny dosažením krajní hodnoty. Tyto filtry se spustí poprvé když je překročena prahová hodnota a znova pak, když už dále není dosahováno prahové hodnoty. Tím poskytují informaci o trvání každé změny v charakteru provozu.

Metoda 5 - SYN Flood (záplava SYN)

Jedním z nejběžnějších typů DoS útoků je SYN Flood. Tento útok může být spuštěn z jednoho nebo více zařízení útočníka a znemožnit přístup na cílový server. Útok využívá mechanismu používaného k založení TCP spojení. Každé TCP spojení vyžaduje před přenosem dat kompletní trojcestné "podání ruky" (three-way handshake):
- **Connection Request** (požadavek na spojení) - První paket (SYN) zaslaný od požadovatele na server odstartuje three-way handshake.
- **Request Acknowledgement** (rozpoznání požadavku) - Druhý paket (SYN + ACK) je poslán serverem požadovateli.
- **Connection Complete** (kompletace spojení) - Třetí paket (ACK) odeslaný požadovatelem zpět na server dokončí three-way handshake.

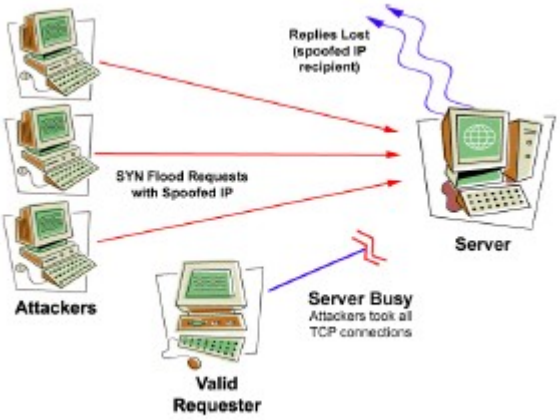
Útok sestává ze záplavy neplatných SYN paketů s falešnou zdrojovou IP adresou. Falešná zdrojová IP adresa způsobí, že cílový server odpovídá na SYN posíláním SYN-ACK na nepodezřívané nebo neexistující zdrojové zařízení. Cílový server pak čeká na zaslání ACK paketu od zdroje ke kompletaci spojení. ACK však nikdy nepřijde a nedokončí tak tabulku spojení s nevyřízeným požadavkem na spojení, které se nikdy nezkompletuje. Tabulka se rychle zaplní

a spotřebuje všechny dostupné zdroje falešnými požadavky. Zatímco počet vstupních spojení se může server od serveru lišit, tabulky mohou být zaplněny pouhými stovkami až tisíci požadavky. Výsledkem je odepření služby - denial of service - jakmile je tabulka plná, cílový server nemůže vyhovět legitimním požadavkům.

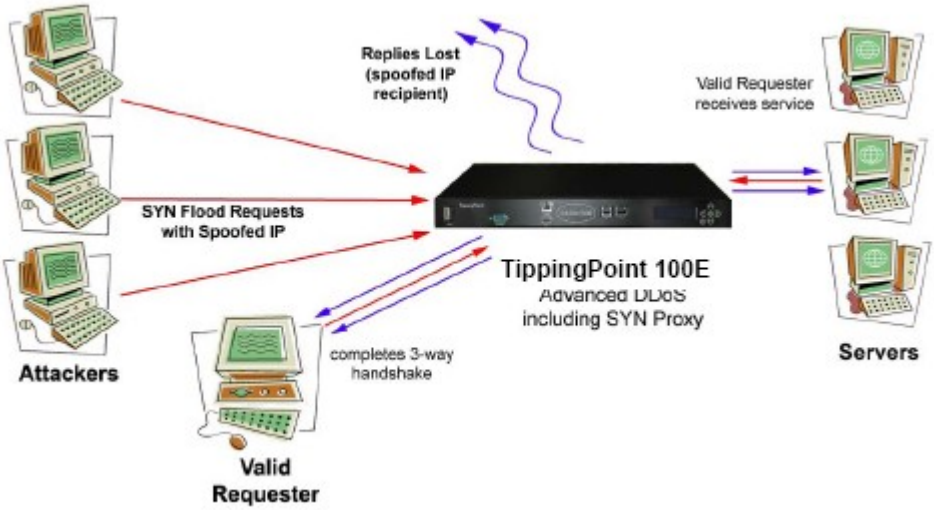
SYN Floods jsou jedním z nejstarších DoS útoků v historii. TCP SYN Flood může zahájit jakákoliv informovaná osoba, což činí tento útok jedním z nejběžnějších. Bez patřičné ochrany se může organizace ocitnout v riskantní situaci. Jak DoS útok bombarduje síť, požadavky rychle zaplní tabulku spojení většiny zařízení síťové bezpečnosti. TippingPoint 100E odstraňuje provoz DoS útoku ze sítě - TippingPoint 100E odstraňuje požadavky z tabulky spojení okamžitě, jako v případě TCP SYN Flood.

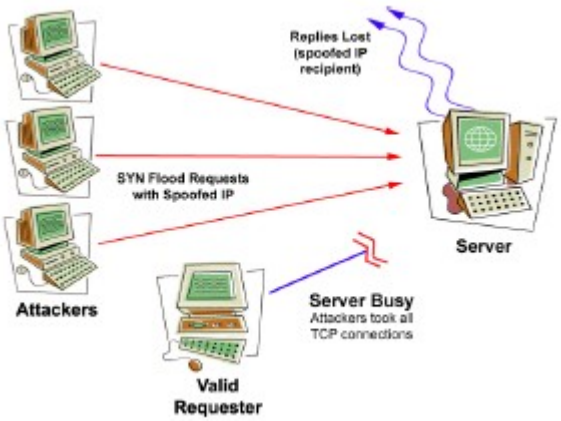
Problém se SYN útoky je v tom, že každý požadavek samostatně vypadá nezhoubně. Falešný požadavek je velmi těžké rozpoznat od legitimního.

Obrázek 1: SYN Flood útok



Obrázek 2: Potlačení SYN Flood útoku s Proxy serverem





Doplněk TippingPointu 100E s pokročilou DDoS ochranou (včetně SYN Proxy filtrů) brání SYN Flood útoku ve spotřebování všech TCP spojení na serveru. Legální požadavek může dokončit three-way handshake.

TippingPoint řešení pro SYN Floods

TippingPoint 100E používá pokročilé metody detekce a ochrany podnikových sítí před SYN Flood. IPS se chová jako proxy - vytváří a odesílá SYN/ACK pakety zpět do místa původu a čeká na finální ACK paket. Poté, co IPS obdrží ACK paket z místa původu, IPS "přehraje" trojcestnou sekvenci příjemci. Úplný scénář útoku a odpovědi je následující:
1. Útočník pošle SYN paket do cíle. TippingPoint 100E zachytí SYN a určí, zda TippingPoint ochrání cíl
2. Pokud ano, IPS vytvoří SYN-ACK namísto cíle.
3. Když IPS obdrží finální ACK trojcestného handshake, IPS ověří pomocí pokročilých algoritmů, že tento paket je odpovědí na SYN-ACK vygenerovanou IPS. Pokud ano, IPS vytvoří spojení s cílem.
4. Jakmile jsou obě spojení vytvořena, TippingPoint udržuje data a spojení a zajišťuje bezpečný provoz. Pokud původce útoku nezkompletuje 3-way handshake, žádné pakety nejsou odeslány do cíle a na TippingPoint IPS není udržován žádný stav.
V případě SYN Flood je respondent plně chráněn před útokem tím, že TippingPoint 100E sleduje, detekuje a blokuje záplavu SYN. TippingPoint umožňuje uživateli označovat klienty jako důvěryhodné. Spojení od důvěryhodných zdrojů nejsou nikdy zastupována.

Když TippingPoint detekuje DoS útok, spustí řadu akcí a hlášení podle uživatelského nastavení. Administrátoři mohou nastavit, aby systém blokoval, povoloval nebo generoval hlášení pro systém, uživatele a logy. Každý filtr v IPS poskytuje ochranu před širokou škálou útoků. Administrátoři sítě si mohou přizpůsobit nastavení filtrů, včetně následujících:
- Akce pro odpovědi na útoky
- Kontakty pro hlášení upozornění
- Výjimky pro určité IP adresy

Metoda 6 - Established Connection Flood (záplava založených spojení)

Záplava založených spojení je dalším vývojovým článkem SYN Flood útoků, které využívají množství zombies ke spáchání DDoS útoku na cíl. Zombies budují zdánlivě legitimní spojení k cílovému serveru. Pomocí velkého počtu zombies, z nichž každá vytváří velký počet spojení s cílem, může útočník

vytvořit tolik spojení, že cíl není nadále schopen přijímat legitimní požadavky na spojení. Například pokud tisíc zombies vytvoří tisíc spojení s cílovým serverem, server musí udržovat milión otevřených spojení. Tento efekt je podobný SYN Flood útoku, ve kterém jsou spotřebovány zdroje serveru, ale tento způsob se mnohem obtížněji detekuje.

Útoky záplavou založených spojení patří mezi útoky, které se nejhůře detekují a blokují. Tyto útoky pocházejí od IP adresy, která byla zkontrolována a přijata proxy serverem přes three-way handshake.

Jakmile útok záplavou založených spojení vstoupí do sítě, zaútočí na proxy server s cílem způsobit jeho zhroucení. Jakmile se proxy zhroutí, přístup do systémů a na servery za proxy serverem je zablokován.

TippingPoint řešení pro záplavy založených spojení

TippingPoint filtry pro záplavu založených spojení sledují množství spojení, která má každý zdroj s chráněným serverem. Jakmile se zdroj pokusí založit více než určený počet spojení s chráněným serverem, budou nová spojení blokována, dokud zdroj některá spojení neukončí. TippingPoint dokáže například zajistit, aby žádný jednotlivý zdroj nevytvořil více než 10 otevřených spojení se serverem. Tím pádem tisíc zombies nemůže vytvořit víc než deset tisíc spojení s chráněným serverem.

Metoda 7 - Connections Per Second Floods (záplavy spojení za sekundu)

Connections Per Second (CPS) Floods útočí na servery velkým rozsahem spojení od zdánlivě platného zdroje. Při těchto útocích se útočník nebo armáda zombies pokouší vyčerpat zdroje serveru rychlým nastavováním a rušením TCP spojení, možná i iniciací požadavku na každé spojení. Útočník například může použít svou armádu zombies k opakovanému načítání domovské stránky z cílového webového serveru. Výsledná zátěž extrémně zpomalí server.

TippingPoint řešení pro CPS záplavy

TippingPoint umožňuje administrátorovi sítě vytvořit CPS filtry. Každý filtr omezuje rozsah počtu spojení, která klient může za sekundu otevřít s příslušným serverem. Každý filtr obsahuje nastavenou prahovou hodnotu vypočítaného průměrného počtu spojení za sekundu, povolených konkrétnímu klientovi. Administrátor sítě může vytvořit CPS filtr pro provoz z portu A do portu B a současně i pro provoz z portu B do portu A. Flexibilní nastavení umožňuje úpravy podle vlastních představ pro příchozí i odchozí provoz a detekci útoků na základě potřeb provozu na síti. TippingPoint počítá s průměrem desetisekundového okna pro umožnění normální fluktuace provozu. Charakter běžného provozu znamená, že webový prohlížeč otevře 10 spojení pro stažení komplexní stránky, pak nečinně čeká, zatímco uživatel čte. Pro přizpůsobení se tomuto charakteru provozu filtry prohlížejí a detekují množství nových spojení zprůměrovaných na 10-ti sekundový interval. Například pokud filtr předepisuje maximálně 3,5 spojení za sekundu, prohlížeče mohou otevřít až 35 spojení za sekundu. Nicméně po vytvoření těchto spojení není prohlížeč schopen otevřít další po dobu dalších 9 sekund. Je to následkem toho že prohlížeč, po 10-ti sekundovém intervalu, dospěl k průměru 3,5 povolených spojení za sekundu. Při použití ve spojení s

filtry pro záplavu založených spojení dokáže ochrana před CPS záplavami poskytovat účinnou detekci a ochranu sítě.

Případová studie - eNom

Společnost eNom, Inc. byla založena v roce 1997 a je jednou z největších ICANN akreditovaných registrátorů doménových jmen s více než čtyřmi milióny jmény. Tato společnost byla vystavena kontinuálním DoS útokům proti svým serverům a zákazníkům. Podle eNomu byly jejich systémy vystaveny DDoS útokům 15 dní v měsíci každý měsíc, od ledna do srpna 2004. Při revizi provozu na síti se zjistilo, že servery obdržely 6000 až 7000 útočných SYN za sekundu. Vrchol útoků proti systému činil asi 40.000 útočných SYN za sekundu.
K ochraně svých zákazníků a síťových systémů společnost hledala systém prevence průniků, který bude detekovat a blokovat útoky bez přerušení legálního provozu. Tváří v tvář obtížnosti a nákladnosti problému, eNom vyhledal skupinu výrobců IPS systémů vybavených ochranou před Denial of Service. Následující seznam obsahuje výrobce, kteří byli vzati v úvahu pro vyřešení ochrany a bezpečnosti:

- TippingPoint
- Radware
- Top Layer
- NAI
- Netscreen

eNom ocenil TippingPoint 100E IPS systém s pokročilou ochranou před Denial of Service (DoS). Pokročilá ochrana před DoS spolu s nejlepší možnou ochranou sítě, aktualizací Digitální vakcíny a výjimečnou technickou podporou činila z TippingPointu řešení, které potřebovali pro zajištění nepřerušovaných služeb pro své zákazníky. Pokročilá DoS ochrana blokovala nejrůznější DoS a DDoS útoky včetně SYN Floods, connection floods, packet floods a obtížně detekovatelných útoků pocházejících od falešných i nefalešných zdrojů.
"Při našem hodnocení předních DoS produktů, představoval TippingPoint to nejlepší. Vždy blokoval nejrůznější DoS útoky mířené na naší síť." Jim Beaver, VP Operations, eNom

>IPS "musí mít"

Pro co nejúplnější ochranu sítě by IPS měl být vybaven základními schopnostmi. Následující tabulka podrobně rozepisuje tyto vlastnosti podle společností, které systémy prevence průniků vyrábějí. TippingPoint vybavuje své oceňované produkty a služby všemi vlastnostmi, které IPS "musí mít".

Attributes	TippingPoint	McAfee	ISS	Juniper	radware	Top Layer
Custom ASICs	Y	8 Celerons	software	software	Y	Y
50Mbps - 5 Gbps	5 Gbps	2Gbps	1Gbps	500M	3Gbps	2Gbps
Switch-like latency	Y	N	N	N	Y	Y
Inline Attack Blocking	Y	Y[1]	Y[1]	Y	Limited	Limited
Bandwidth Management	Y	N	N	N	Y	N
DDoS SYN Flood Protection	Y	N	N	Y	Y	Y
DDoS Connection Rate Limits	Y	N	N	N	N	Y
Filter Method: Signature	Y	Y	Y	Y	Y	N
Filter Method: Protocol	Y	Y	Y	Y	N	Limited
Filter Method: Vulnerability	Y	Y	Y	Limited	N	N
Filter Method: Traffic Anomaly	Y	Y	N	N	N	Limited
VoIP Protection	Y	N	N	N	N	N

[1] Rarely deployed inline, usually as IDS

Pro získání plné ochrany před DoS útoky organizace typicky potřebují při svém růstu zakoupit více proxy serverů, síťových bezpečnostních zařízení, systémů prevence průniků, stejně jako softwarových balíčků, aktualizací a rozšířených licencí.

TippingPoint odpovídá těmto požadavkům jediným systémem. TippingPoint je jednoduché, cenově dostupné a škálovatelné řešení, vybavené širokou škálou mechanismů ochrany, včetně filtrů anomálií aplikací a protokolů, filtrů pro šifrování, filtrů statistických anomálií provozu, filtrů prahových hodnot špiček provozu a pokročilých DoS/DDoS filtrů pro detekci a blokování útoků. Útoky pokračují, vyvíjejí se a jejich důmyslnost vzrůstá. Flexibilita platformy TippingPointu nabízí aktuální úroveň ochrany před současnými útoky a potenciál pro ochranu před budoucími útoky.