Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Ochrona przed atakami Check Point DDoS Protector™

W ciągu sekundy zatrzymuj ataki Denial of Service dzięki konfigurowalnej, wielowarstwowej ochronie blokującej szeroki zakres zagrożeń

Urządzenia Check Point DDoS Protector

Na dzisiejszej mapie zagrożeń ataki odmowy usługi„Denial of Service" (DoS), zyskują na ilości, szybkości i skomplikowaniu. Ataki Denial of Service oraz Distributed Denial of Service (DDoS) są stosunkowo łatwe do przeprowadzenia i mogą spowodować poważne szkody dla przedsiębiorstw polegających w swojej działalności na usługach webowych. Liczne (ponad 50) zestawy ułatwiające tworzenie ataków DDoS (tzw. toolkity) są łatwo dostępne w Internecie. Ponadto w ponad 230 krajach obserwuje się wzrost liczby tych właśnie ataków. Ataki DDoS często motywowane są chęcią zysku: w roku 2011 cyberprzestępcy zyskali przy ich użyciu oszałamiającą sumę 12,5 miliarda dolarów. W roku 2012 natomiast obserwuje się niepokojąco szybki wzrost zagrożeń DDoS wymierzonych w sektor usług finansowych. Niemniej jednak najpopularniejszą areną dla ataków Denial of Service staje się działalność hackerska mająca na celu manifestację poglądów politycznych (tzw. hacktivism) lub też związana z politycznymi motywacjami. Najlepszym przykładem jest tutaj działalność grupy Anonymous, która przeprowadziła skuteczne serie ataków odwetowych w związku z oświadczeniami, z którymi grupa się nie zgadza. Ataki te wymierzone były w osoby indywidualne, organizacje, instytucje państwowe oraz kraje.

Wiele rozwiązań ochrony DDoS wdrażanych jest przez dostawców usług internetowych (ISP). Oferują one ogólne zabezpieczenia przeciw atakom w warstwie sieciowej. Należy zwrócić jednak uwagę, że dzisiejsze ataki DDoS są o wiele bardziej złożone i składają się z serii pomniejszych ataków wymierzonych w sieci i aplikacje. Skuteczne rozwiązania DDoS powinny pozwalać przedsiębiorstwom na dostosowywanie zabezpieczeń odpowiednio do zmieniających się potrzeb bezpieczeństwa, szybkie reagowanie w razie ataku oraz na korzystanie z różnorodnych opcji implementacji.

OPIS PRODUKTU

Nowe rozwiązanie Check Point zapewniające ochronę przed atakami DDoS, DDoS Protector, pozwala biznesowi skorzystać z wielowarstwowych, dostosowywanych zabezpieczeń oraz wydajności na poziomie 12 Gb/s. Zabezpieczenia te zapewniają automatyczną ochronę przed atakami typu network flood oraz przed atakami warstwy aplikacji. Możliwa jest dzięki temu szybka reakcja na złożone ataki Denial of Service dnia dzisiejszego. Urządzenia DDoS Protector oferują elastyczne opcje wdrożenia, które w prosty sposób umożliwią objęcie ochroną przedsiębiorstw każdej wielkości. Zapewniają one również zintegrowany system zarządzania bezpieczeństwem pozwalający na analizę ruchu sieciowego w czasie rzeczywistym, jak również udostępniają informacje na temat zarządzania zagrożeniami w celu zaawansowanej ochrony przed atakami DDoS. Check Point dostarcza również zasoby techniczne oraz obsługę w trybie 24/7 w celu zapewnienia najbardziej aktualnych zabezpieczeń.

KLUCZOWE WŁAŚCIWOŚCI

- Zapewnia ochronę przed znanymi i nieznanymi atakami DDoS
- Chroni przed atakami sieciowymi oraz atakami aplikacyjnymi
- Elastyczne mechanizmy filtrujące wykrywają exploity i zapobiegają powiązanym atakom
- Zapewnia ochronę przed atakami HTTP
- Zapewnia ochronę przed atakami mającymi na celu radykalne ograniczenie przepustowości (bandwidth flood)
- Mechanizmy szybkiego tworzenia niestandardowych sygnatur zapewniają ciągłość procesów biznesowych

KLUCZOWE KORZYŚCI

- Zapewnia ochronę przed ewoluującymi atakami DDoS w celu minimalizowania wpływu na działalność biznesową
- Zaawansowane technologie umożliwiają podtrzymanie usług webowych w czasie ataku
- Urządzenie dostarczane jest jako rozwiązanie „out of the box"i jest przygotowane do natychmiastowego działania
- Integracja z zarządzaniem bezpieczeństwa Check Point w celu uzyskania większej widoczności oraz kontroli systemów
- Rozwiązanie DDoS o wysokiej wydajności: 14Gb/s pojemności łącza oraz 12Gb/s przepustowości
- Wielowarstwowy system ochrony powstrzymujący ataki różnorodnego typu
- Zabezpieczenia mogą być dostosowywane do wielkości przedsiębiorstwa oraz jego potrzeb związanych z bezpieczeństwem
- Elastyczne opcje wdrożenia umożliwiają instalację na miejscu lub poprzez dostawcę usług internetowych

softwareblades™

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

WIELOWARSTWOWE ZABEZPIECZENIA

Zabezpieczenia sieci oraz przesyłanych danych przed atakami flood

Ochrona przed atakami DDoS wymierzonymi w sieci z wykorzystaniem następujących elementów:

Behawioralna analiza DoS (Behavioral DoS) – Chroni przed atakami TCP, UDP, ICMP, IGMP oraz fragmentarycznymi atakami DDoS dzięki systemom wykrywania bazującym na adaptacyjnej analizie behawioralnej.

System DoS Shield – Chroni przed znanymi narzędziami wykorzystywanymi do ataków DDoS dzięki predefiniowanym i odpowiednio dostosowanym filtrom. Filtry te blokują limity częstotliwości na podstawie wzorca.

Ochrona Syn (Syn Protection) – Blokuje ataki DoS bazujące na spoofingu SYN stosując odpowiednie progi częstotliwości zapytań SYN dla każdego serwera objętego ochroną.

Czarna lista (Black List) – Blokuje ogólne ataki za pomocą reguł klasyfikacji i przedawnienia dla kanałów komunikacji źródło-punkt docelowy stosowanych w warstwie 3 i 4.

Limity przepustowości łącza (Connection Rate Limit) – Blokuje ogólne ataki flood dla niewspieranych protokołów (spoza DNS, HTTP) oraz dla warstwy aplikacji, stosując progi przepustowości łącza.

Zabezpieczenia przed atakami DoS/DDoS wymierzonymi w aplikacje

Wykorzystuje następujące elementy ochrony przed bardziej złożonymi atakami DDoS oraz nadużyciami zasobów aplikacyjnych:

Ochrona Syn (Syn Protection) za pomocą technologii Web Challenge – Chroni przed atakami DoS bazującymi na połączeniu HTTP stosując odpowiednie progi częstotliwości zapytań SYN dla każdego serwera objętego ochroną.

Behawioralne zabezpieczenia DNS – Blokuje ataki DoS bazujące na wysyłaniu zapytań DNS. Stosuje do tego mechanizmy wykrywania za pomocą adaptacyjnej analizy behawioralnej. Mechanizmy te wykorzystują limity ograniczające footprint DNS oraz techniki DNS wyzwania i odpowiedzi.

Behawioralne zabezpieczenia HTTP (tzw. „HTTP Mitigator") – Blokuje ataki wykorzystujące połączenia HTTP oraz ataki ograniczające przepustowość uploadu danych poprzez HTTP. Wykorzystuje w tym celu techniki wykrywania na podstawie adaptacyjnej analizy behawioralnej HTTP dla serwera, footprint HTTP za pomocą webowych technik wyzwanie-odpowiedź, przekierowania według kodu odpowiedzi 302 oraz wyzwania JS.

Kierowane zabezpieczenia przed atakami DoS/DDoS dla aplikacji

Zapobiega atakom DoS oraz DDoS, które wymagają specjalnych kryteriów filtrowania. Elastyczne definicje filtrowania poszukują określonych wzorców zawartości w każdym pakiecie. Umożliwia analizowanie i blokowanie przeprowadzanych ataków poprzez dynamiczne definiowanie zabezpieczeń.

ZARZĄDZANIE

Urządzenia DDoS zintegrowane są z system zarządzania bezpieczeństwem Check Point, który obejmuje następujące elementy:

SmartEvent
Skonsolidowane rozwiązanie monitorowania zdarzeń bezpieczeństwa i ich analizy, które w czasie rzeczywistym dostarcza informacje zarządzania. Umożliwiają one natychmiastowe powstrzymywanie zagrożeń oraz blokowanie ataków za pomocą dynamicznie definiowanych zabezpieczeń. System pozwala przechodzić z widoku procesów biznesowych do analizy danych za pomocą jedynie trzech kliknięć myszką.

SmartLog
Zaawansowane narzędzie analizowania logów, które w proaktywny sposób dostarczają informacje wywiadowcze. Wyniki wyszukiwania na podstawie jakiegokolwiek pola w logu dostarczane są w ułamku sekundy. Umożliwia to natychmiastowy wgląd w informacje zawarte w miliardowych zbiorach logów zgromadzonych na przestrzeni licznych okresów czasu oraz dla licznych domen.

SmartView Tracker
Kompleksowe rozwiązanie audytowe, które służy do analizy problemów systemowych oraz zagadnień bezpieczeństwa, gromadzenia informacji dla celów prawnych lub audytowych oraz generowanie raportów w celu analizy profili transmisji.
W wypadku ataku lub innej podejrzanej aktywności sieciowej SmartView Tracker może być wykorzystany do tymczasowego lub definitywnego przerwania połączenia z określonego adresu IP.

Alarmy

SNMP V1, 2C oraz 3, plik logu, Syslog, Email

Konfiguracja

SNMP, V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, SOAP, API, Konsola (zgodnie z wyborem użytkownika).

Synchronizacja czasu

Zgodnie z protokołem Network Time Protocol (NTP).

Eksport w czasie rzeczywistym informacji na temat sygnatury

Interfejs XML typu northbound eksportuje parametry behawioralne.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SPECYFIKACJA

Model urządzenia DDoS Protector	506	1006	2006	3006	4412	8412	12412
Klasa sieci	Enterprise				Datacenter		
Wydajność[1]							
Pojemność[2]	500Mb/s	1Gb/s	2Gb/s	3Gb/s	4Gb/s	8Gb/s	14Gb/s
Przepustowość[3]	500Mb/s	1Gb/s	2Gb/s	3Gb/s	4Gb/s	8Gb/s	12Gb/s
Maks. liczba równoczesnych sesji	2,000,000	2,000,000	2,000,000	2,000,000	4,000,000	4,000,000	4,000,000
Maks. wydajność zapobiegania atakom DDoS Flood (liczba pakietów na sekundę)	1,000,000	1,000,000	1,000,000	1,000,000	10,000,000	10,000,000	10,000,000
Opóźnienie	<60 mikrosekundy						
Sygnatury w czasie rzeczywistym	Wykrywanie ataków i zapewnienie ochrony w czasie poniżej 18 sekund						
Porty inspekcji							
10/100/1000 miedziany Ethernet	4	4	4	4	8	8	8
GbE (SFP)	2	2	2	2	4	4	4
10GbE (XFP)	–	–	–	–	4	4	4
Porty zarządzania							
10/100/1000 miedziany Ethernet	2	2	2	2	2	2	2
RS-232	1	1	1	1	1	1	1
Tryb operacyjny							
Obsługa sieci	Transparentna transmisja L2						
Tryby wdrożenia	In-line; monitoring portu span; monitoring portu copy; local out-of-path; out-of-path mitigation						
Obsługa protokołów tunelowania	VLAN Tagging, L2TP, MPLS, GRE, GTP						
IPv6	Obsługuje sieci IPv6 i blokuje ataki IPv6						
Działanie polityki	Blokuj i raportuj; Tylko raportuj						
Działania blokujące	Porzuć pakiet, reset (źródło, punkt docelowy, oba), zawieś (źródło, port źródłowy, punkt docelowy, port docelowy lub jakakolwiek kombinacja wymienionych); Wyzwanie-Odpowiedź dla ataków HTTP oraz DNS						
Wysoka dostępność							
Tryb Fail-open / Fail-close	Wewnętrzny fail-open/fail-close dla portów miedzianych; wewnętrzny fail-close dla portów SFP; opcjonalny fail-open dla portów SFP 4				Wewnętrzny fail-open/fail-close dla portów miedzianych; wewnętrzny fail-close dla portów SFP i XFP; opcjonalny fail-open dla portów SFP i XFP 5		
SKU	CPAP-DP506	CPAP-DP1006	CPAP-DP2006	CPAP-DP3006	CPAP-DP4412	CPAP-DP8412	CPAP-DP12412

[1] Faktyczne parametry wydajności mogą się zmieniać w zależności od konfiguracji sieci, rodzaju przesyłanych danych, etc.
[2] Pojemność mierzona jest jako maksymalna zdolność transmisji przy braku skonfigurowanych profili bezpieczeństwa
[3] Przepustowość jest mierzona za pomocą zabezpieczeń behawioralnych oraz zabezpieczeń sygnaturowych przy użyciu profilu ochrony eCommerce
[4] Zewnętrzny przełącznik światłowodowy fail-open z portami SFP dostępny jest za dodatkowa opłatą
[5] Zewnętrzne przełączniki światłowodowe fail-open z portami SFP lub XFP dostępne są za dodatkową opłatą

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Akcesoria DDoS Protector	SKU
Dołączalny światłowód (XFP) jednomodowy 10Gb/s	LR CPAC-DP-10LR-XFP
Dołączalny światłowód (XFP) wielomodowy 10Gb/s	SR CPAC-DP-10SR-XFP
Dołączalny światłowód jednomodowy 1Gb/s	ZX CPAC-DP-1ZX-SFP
Dołączalny przewód miedziany 1000BASET 1Gb/s	CPAC-DP-1C-SFP
Dołączalny światłowód jednomodowy 1Gb/s	LX CPAC-DP-1LX-SFP
Dołączalny światłowód wielomodowy 1Gb/s	SX CPAC-DP-1SX-SFP
Zewnętrzna jednostka bypass 10GbE obsługująca jeden (1) segment LR – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-1LR-10BP
Zewnętrzny chassis bypass 10GbE zawierający jeden segment LR, który może zostać rozszerzony do czterech (4) segmentów – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-4LR-10BP
Zewnętrzny moduł bypass 10GbE, segment interfejsu LR – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-1LR-10BPM
Zewnętrzny chassis bypass 10GbE zawierający jeden segment interfejsu SR, który może zostać rozszerzony do czterech (4) segmentów – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-4SR-10BP
Zewnętrzny moduł bypass 10GbE, segment interfejsu SR – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-1SR-10BPM
Zewnętrzna jednostka bypass 1GbE obsługująca jeden (1) segment SX – zabezpieczenie na wypadek awarii zasilania oraz łącza – dla serii urządzeń DDoS Protector x412	CPAC-DP-1SX-1BP
Zewnętrzna jednostka bypass 1GbE obsługująca jeden (1) segment LX do SX – dla serii urządzeń DDoS Protector serii x412	CPAC-DP-1LX-1BP
Dwugniazdowa rama montażu w racku dla przełączników bypass	CPAC-DP-2RM
Podwójny zasilacz DC dla urządzeń DDoS Protector serii x412	CPAC-DP-2PS-DC
Pojedynczy zasilacz DC dla urządzeń DDoS Protector serii x412	CPAC-DP-PS-DC

Dystrybucja w Polsce:

CLICO

CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 12 378-37-00
tel. 12 632-51-66
tel. 12 292-75-22... 24
fax 12 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 32 444-65-11
tel. 32 203-92-35
tel. 32 609-80-50…51
fax 32 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 22 201-06-88
tel. 22 518-02-70...75
fax 22 518-02-73
e-mail: warszawa@clico.pl

7 lipiec, 2012