KASPERSKY DDOS PROTECTION

Dowiedz się, jak działa Kaspersky DDoS Protection

► CYBERPRZESTĘPCY ATAKUJĄ FIRMY

Jeśli Twoja firma kiedykolwiek padła ofiarą ataku DDoS (Distributed Denial of Service), z pewnością wiesz, że koszty finansowe i dotyczące reputacji w wyniku takiego incydentu mogą być ogromne. Jednak nawet jeśli Twoja firma miała szczęście i udało jej się nie trafić na celownik cyberprzestępców czy hakerów, którzy przeprowadzają takie ataki, przyszłość może już nie wyglądać tak dobrze.

WZRASTA LICZBA I SIŁA ATAKÓW

Niestety, w ostatnich latach koszt przeprowadzenia ataku DDoS znacznie się zmniejszył – to oznacza, że ma miejsce więcej ataków niż kiedykolwiek wcześniej. Jednocześnie, obecne ataki charakteryzują się większą złożonością i przeprowadzane są na skalę, która może w ciągu zaledwie kilku sekund nadwyrężyć łącza komunikacyjne atakowanej firmy – niemal natychmiast osłabiając istotne wewnętrzne procesy biznesowe i doprowadzając do całkowitego odłączenia atakowanej firmy od internetu.

Ponieważ firmy, niezależnie od rozmiaru, polegają na swojej infrastrukturze IT oraz stronach internetowych, wykonując istotne dla swojej działalności procesy, długi czas przestoju – który może być wynikiem ataku DDoS – to problem, na który nie mogą sobie pozwolić. Biorąc pod uwagę liczbę, skalę i siłę współczesnych ataków, żadna firma nie może odkładać kwestii ochrony przed atakami DDoS i łagodzenia ryzyka do czasu, gdy jej infrastruktura zostanie zaatakowana. Zamiast tego, firmy – jak również organizacje sektora publicznego – muszą być świadome zagrożeń i zapewnić sobie odpowiednie środki ochrony przed atakami DDoS.

LEPIEJ ZAPOBIEGAĆ NIŻ LECZYĆ

Każda firma powinna posiadać strategię ochrony przed incydentami DDoS – którą może „wcielić w życie”, jak tylko zostanie wykryty atak. Wówczas, w przypadku takich działań cyberprzestępczych, firma będzie mogła niezwłocznie złagodzić skutki ataku, aby:

- Skrócić czas przerwy w działaniu kluczowej dla działalności infrastruktury oraz procesów.
- Zapewnić klientom możliwość dalszego dostępu do usług online.
- Utrzymać produktywność pracowników.
- Zminimalizować szkody na reputacji.

► METODY PRZEPROWADZANIA ATAKÓW DDoS

Cyberprzestępcy i hakerzy stosują wiele różnych technik w celu przeprowadzania ataków DDoS, które paraliżują lub przeciążają infrastrukturę IT atakowanej firmy.

ATAKI WOLUMETRYCZNE

Tego rodzaju ataki stają się coraz powszechniejsze. W wyniku wygenerowania ruchu, którego ilość jest większa niż przepustowość firmy, zostaje wykorzystany limit połączenia internetowego atakowanej organizacji, co powoduje wstrzymanie lub opóźnienie wszystkich działań online.

ATAKI NA WARSTWĘ APLIKACJI

Celem ataków w warstwie aplikacji jest spowodowanie awarii serwerów, które obsługują istotne aplikacje – takich jak serwery sieciowe, od których zależy obecność firmy w internecie.

ATAKI NA INFRASTRUKTURĘ

Ataki przeprowadzane w celu wyłączenia sprzętu sieciowego oraz / lub systemów operacyjnych serwerów mogą całkowicie zatrzymać działanie kluczowych procesów biznesowych.

ATAKI HYBRYDOWE

Cyberprzestępcy przeprowadzają również złożone ataki, które łączą kilka metod.

▶ WSZECHSTRONNE ROZWIĄZANIE DO OCHRONY PRZED ATAKAMI I NEUTRALIZOWANIA ICH SKUTKÓW

Kaspersky DDoS Protection to rozwiązanie zapewniające wszechstronną, zintegrowaną ochronę przed atakami DDoS oraz neutralizowanie ich skutków, które działa na każdym etapie niezbędnym w celu zabezpieczenia Twojej firmy. Od ciągłej analizy całego firmowego ruchu online poprzez ostrzeżenia o potencjalnym ataku, przyjęciu ruchu przekierowanego z Twojej firmy, przefiltrowaniu go i zwróceniu Ci „czystego" ruchu, Kaspersky DDoS Protection oferuje wszystko, czego potrzebuje Twoja firma, aby zapewnić sobie ochronę przed wszystkimi rodzajami ataków DDoS i usuwać ich skutki.

KASPERSKY DDOS PROTECTION OBEJMUJE:

- Sensor – specjalne oprogramowanie Kaspersky Lab, które działa w obrębie Twojej infrastruktury IT.
- Usługi naszej globalnej sieci centrów czyszczenia ruchu.
- Pomoc świadczoną przez naszych ekspertów z centrum bezpieczeństwa oraz ds. ochrony przed atakami DDoS.
- Szczegółową analizę i raporty po ataku.

▶ JAK DZIAŁA KASPERSKY DDoS PROTECTION

Sensor Kaspersky Lab gromadzi informacje dotyczące całego ruchu danych przepływającego przez firmę – 24 godziny na dobę, siedem dni w tygodniu, 365 dni w roku. Sensor jest zainstalowany możliwie najbliżej zasobu, który ma być chroniony – i nieustannie gromadzi dane dotyczące ruchu, w tym:

- Dane dotyczące nagłówka.
- Typy protokołów.
- Liczba wysyłanych i otrzymywanych bajtów.
- Liczba wysyłanych i otrzymywanych pakietów.
- Działania i zachowanie – każdego, kto odwiedza Twoją stronę internetową.
- Wszystkie metadane dotyczące Twojego ruchu.

Wszystkie te informacje są wysyłane do działających w chmurze serwerów firmy Kaspersky Lab, gdzie są poddawane analizie, na podstawie której możemy stworzyć profil zachowania typowego odwiedzającego oraz profil typowego ruchu firmowego – oraz określić różnice w ruchu ze względu na porę dnia i dzień tygodnia, a także wpływ specjalnych zdarzeń na przebieg ruchu. Dzięki tak szczegółowej analizie „typowych warunków ruchu" w Twojej firmie oraz „typowego zachowania odwiedzających" nasze działające w chmurze serwery potrafią dokładnie ocenić warunki „żywego" ruchu w Twojej firmie w czasie rzeczywistym i szybko zidentyfikować anomalie wskazujące na to, że Twoja firma stała się celem ataku.

Ponadto, nasi eksperci zajmujący się danymi dotyczącymi zagrożeń nieustannie monitorują krajobraz zagrożeń DDoS w celu identyfikowania nowych ataków. Te specjalistyczne dane pomagają nam zapewnić naszym klientom szybką reakcję na każdy rodzaj ataku.

UNIKANIE FAŁSZYWYCH ALARMÓW… A NASTĘPNIE FILTROWANIE RUCHU FIRMOWEGO

Jak tylko nasze serwery lub eksperci ds. analizy danych zidentyfikują potencjalny atak na firmę, centrum bezpieczeństwa Kaspersky Lab otrzyma ostrzeżenie. Aby pomóc firmom uniknąć fałszywych alarmów – i niepotrzebnych zakłóceń w pracy – inżynierowie z Kaspersky Lab sprawdzają, czy anomalia w ruchu lub podejrzane zachowanie nie wynika z ataku DDoS. W takim wypadku, nasi eksperci natychmiast skontaktują się z Twoją firmą – aby zalecić przekierowanie Twojego ruchu do naszej sieci centrów czyszczenia.

Podczas ataku, gdy cały Twój ruch przechodzi przez jedno z naszych centrów czyszczenia:

Twoja infrastruktura nie jest już przeciążona ogromną ilością „śmieciowego ruchu",
nasz proces filtrowania odrzuca cały śmieciowy ruch,
czysty ruch jest z powrotem przesyłany do Twojej firmy – z naszej sieci centrów czyszczenia,
… a cały proces jest całkowicie przezroczysty dla Twoich pracowników i klientów.

▶ SZYBKA I ŁATWA KONFIGURACJA OCHRONY

Jeśli wybierzesz Kaspersky DDoS Protection, będziesz musiał wykonać kilka zadań konfiguracji, aby rozwiązanie zapewniało Ci monitoring 24 godziny na dobę przez 7 dni w tygodniu oraz zostały ustanowione kanały komunikacji o atakach w czasie rzeczywistym. Kaspersky Lab – i jego partnerzy – może wziąć na siebie tak dużą część procesu konfiguracji, jak wymaga Twoja firma.

Jeśli potrzebujesz rozwiązania, które jest „gotowe do działania", Kaspersky Lab i jego partnerzy mogą przeprowadzić ogromną większość procedur konfiguracji – w tym:

- Instalowanie sensora po Twojej stronie.
- Konfigurowanie przekierowywania ruchu do naszych centrów czyszczenia.
- Konfigurowanie dostarczania „czystego" ruchu do Twojej firmy.

W takim wypadku, musisz jedynie zapewnić oddzielny kanał internetowy dla sensora – tak aby Kaspersky DDoS Protection mógł gromadzić dane, gdy Twój główny kanał internetowy zostanie wyłączony na skutek ataku.

SENSOR – UMOŻLIWIA MONITOROWANIE 24 GODZ. NA DOBĘ PRZEZ 7 DNI W TYGODNIU

Sensor Kaspersky Lab jest dostarczany wraz ze standardowym systemem operacyjnym Ubuntu Linux.
Ponieważ sensor to oprogramowanie działające na na standardowym serwerze x86 - lub na maszynie wirtualnej* - nie musisz utrzymywać specjalnego sprzętu. Sensor jest podłączony do portu SPAN (Switched Port Analyzer), dlatego może uzyskać najlepszy z możliwych obrazów ruchu, który płynie do i wypływa z chronionego zasobu.
Jak tylko sensor zostanie podłączony do Twojej infrastruktury, zaczyna gromadzić dane dotyczące Twojego ruchu przychodzącego i wychodzącego. Analizuje nagłówki każdego pakietu i wysyła informacje do opartych na chmurze serwerów Kaspersky DDoS Protection – gdzie tworzymy profile statystyczne „typowego zachowania ruchu" oraz „typowego zachowania odwiedzającego" dla Twojej firmy.
Aby zachować prywatność Twojej komunikacji – i pomóc w zapewnieniu zgodności z przepisami – sensor nie przechwytuje zawartości żadnych wiadomości w Twoim ruchu danych. Gromadzi jedynie dane dotyczące samego ruchu – zatem procesy Kaspersky DDoS Protection nigdy nie naruszają poufności Twoich wiadomości.

*Maszyna wirtualna musi spełniać lub przewyższać minimalne wymagania dotyczące wydajności określone przez Kaspersky Lab.

PRZEKIEROWYWANIE RUCHU

W normalnych warunkach – gdy oparte na chmurze serwery Kaspersky DDoS Protection monitorują ruch w celu zidentyfikowania wszelkich śladów ataku DDoS – Twój ruch jest dostarczany bezpośrednio do Twojej sieci firmowej. Zostaje przekierowany – do naszej globalnej sieci centrów czyszczenia – tylko wtedy, gdy został wykryty atak, a Twoja firma potwierdziła, że chce przekierować swój ruch.

Kaspersky DDoS Protection zapewnia Ci wybór metod przekierowania:

- Border Gateway Protocol (BGP).
- Domain Name System (DNS).

TUNELE WIRTUALNE GRE (GENERIC ROUTING ENCAPSULATION)

Niezależnie od tego, która metoda przekierowania jest najlepsza dla Twojej firmy, tunele wirtualne GRE umożliwiają komunikację pomiędzy Twoją bramą graniczną – lub routerem – oraz każdym centrum czyszczenia Kaspersky DDoS Protection.

W przypadku, gdy Twoja firma padnie ofiarą ataku DDoS, cały Twój ruch może zostać przekierowany do jednego z naszych centrów czyszczenia. Tunele wirtualne GRE są następnie wykorzystywane do dostarczania „czystego" ruchu – z naszych centrów czyszczenia do Twojej firmy.

▶ WYBÓR POMIĘDZY BGP I DNS

To, czy skonfigurujesz przekierowanie swojego ruchu za pośrednictwem BGP czy DNS, zależy w dużej mierze od charakteru infrastruktury IT i komunikacji Twojej firmy:

- W przypadku BGP, musisz posiadać:
sieć niezależną od dostawcy – która obejmuje zasoby podlegające ochronie,
autonomiczny system.
Kryteria te jest w stanie spełnić większość dużych firm.

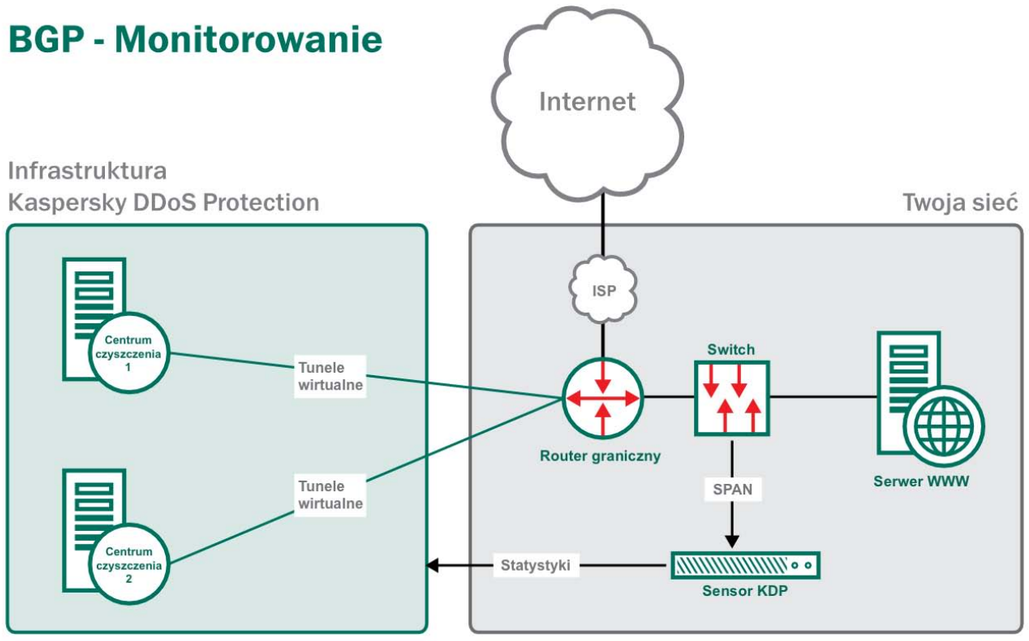
- W przypadku DNS, niezbędne jest, abyś mógł:
zarządzać swoją własną strefą domenową dla zasobów, które chcesz chronić,
ustawić maksymalny czas oczekiwania (TTL) dla wpisów DNS na 5 minut.

Ogólnie, podczas ataku metoda BGP umożliwia szybsze przekierowanie ruchu – dlatego jest ona wybierana przez większość firm.

▶ JAK DZIAŁA PRZEKIEROWANIE BGP

MONITOROWANIE

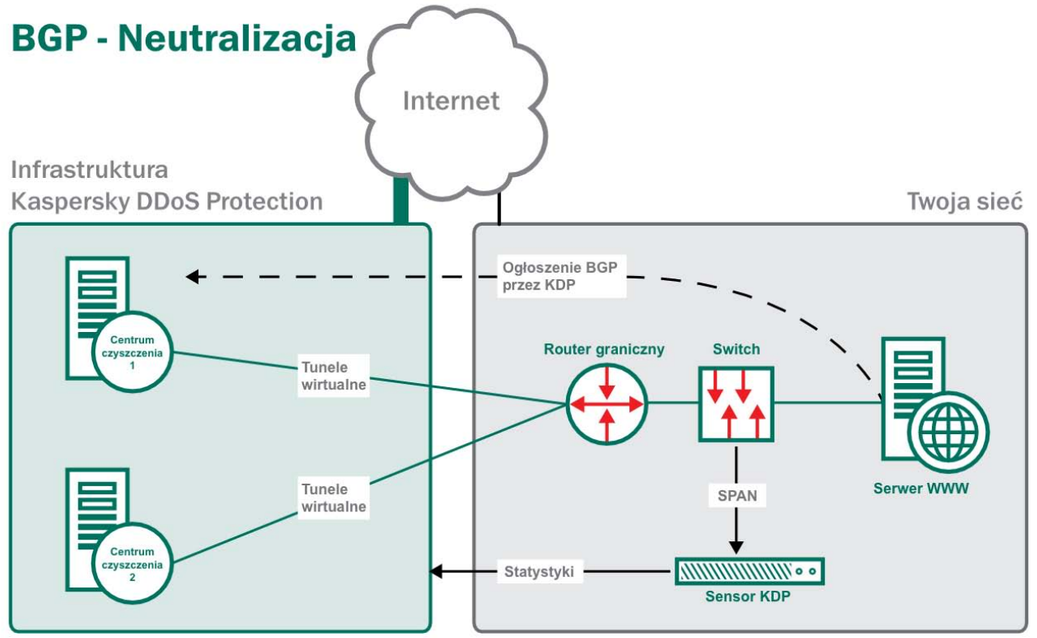
W trybie monitorowania cały Twój ruch jest dostarczany bezpośrednio do Twojej firmy. Jednak tunele wirtualne GRE działają „na żywo" – zarówno Twoje routery jak i nasze routery BGP często wymieniają informacje dotyczące statusu, tak aby centra czyszczenia Kaspersky DDoS Protection były gotowe na otrzymanie ruchu przekierowanego z Twojej firmy, kiedy jest to konieczne.



PODCZAS ATAKU

Kiedy czujnik Kaspersky Lab zidentyfikuje nieprawidłowości w ruchu – a inżynierowie z Kaspersky Lab potwierdzą początek ataku – możesz zdecydować, aby cały Twój ruch został przekierowany do centrum czyszczenia Kaspersky DDoS Protection.

Podczas ataku sensor nadal będzie gromadził informacje i wysyłał je do analizy na opartych na chmurze serwerach Kaspersky DDoS Protection.



PO ATAKU

Po ataku Twój ruch będzie ponownie wysyłany bezpośrednio do Twojej firmy. Sensor nadal będzie gromadził dane dotyczące Twojego ruchu – i nieustannie przekazywał te dane do opartych na chmurze serwerów, tak abyśmy mogli nieustannie udoskonalać nasze profile zachowania względem Twoich typowych warunków ruchu.

Tunele wirtualne pozostają aktywne – wymieniając informacje dotyczące statusu pomiędzy Twoimi routerami a routerami Kaspersky Lab – tak aby Kaspersky DDoS Protection był gotowy do działania, gdy Twoja firma będzie atakowana po raz kolejny, a Ty ponownie zdecydujesz się na przekierowanie swojego ruchu.

Po ataku eksperci z Kaspersky Lab dostarczą również szczegółową analizę oraz raporty określające:

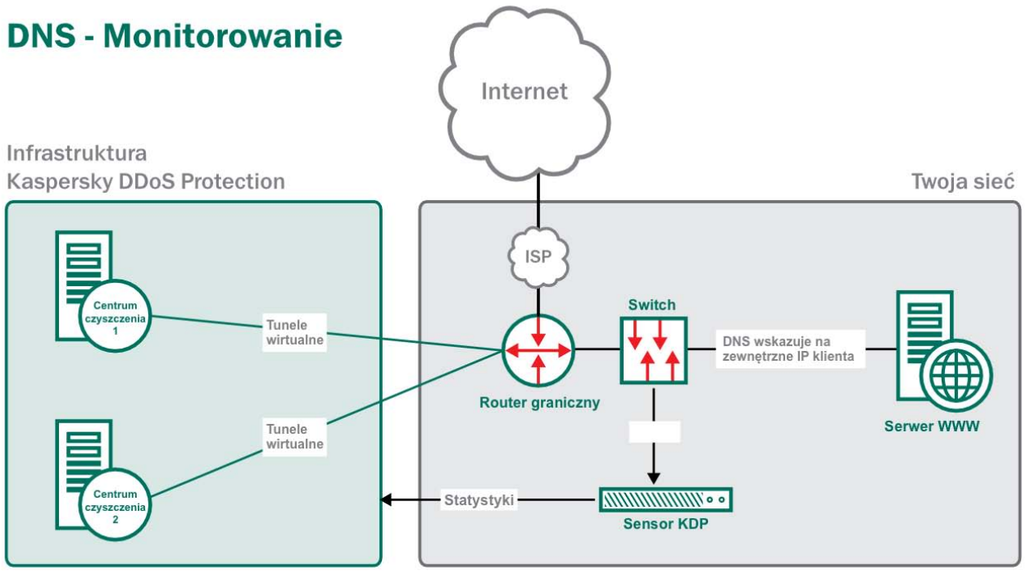
- co stało się podczas ataku,
- jak długo trwał atak,
- w jaki sposób Kaspersky DDoS Protection poradził sobie z atakiem.

▶ JAK DZIAŁA PRZEKIEROWANIE DNS

MONITORING

Podczas wstępnej konfiguracji Kaspersky Lab przydziela Twojej firmie jedną ze swojej puli adresów IP Kaspersky DDoS Protection. Ten adres będzie wykorzystywany w razie ataku.

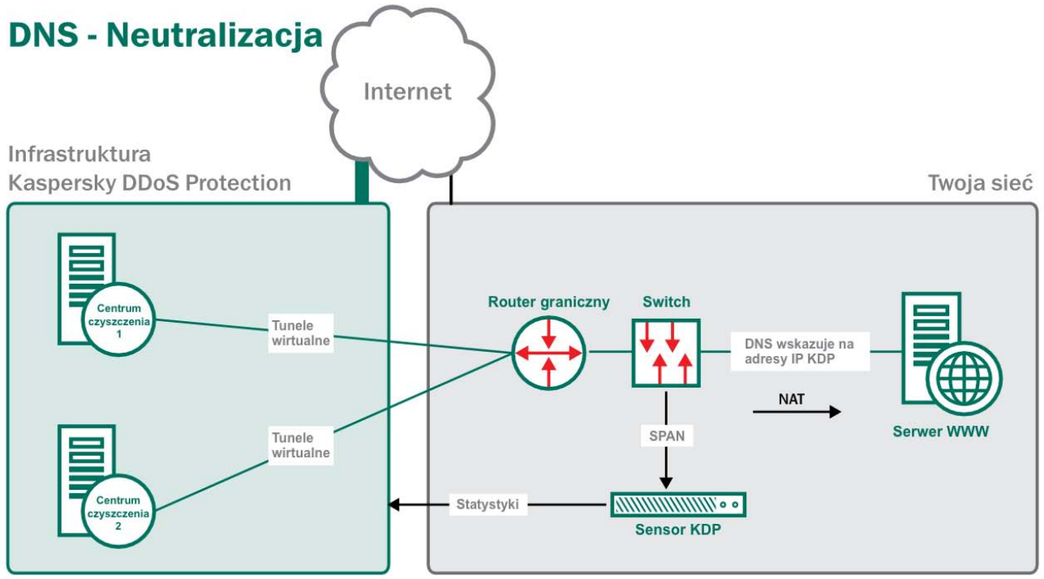
W trybie monitorowania cały Twój ruch jest dostarczany bezpośrednio do Twojej firmy – za pośrednictwem jej standardowego adresu/adresów IP. Jednak tunele wirtualne GRE działają „na żywo" – Twoje routery i nasze routery BGP często wymieniają informacje dotyczące statusu, dzięki czemu centra czyszczenia Kaspersky DDoS Protection były gotowe przyjąć ruch przekierowany z Twojej firmy, jak tylko zaistnieje taka potrzeba.



PODCZAS ATAKU

Gdy sensor Kaspersky Lab zidentyfikuje nieprawidłowości w ruchu – a inżynierowie Kaspersky Lab potwierdzą początek ataku – musisz po prostu zmienić adres IP swojej firmy w rekordzie A serwera DNS, tak aby Twoja firma wykorzystywała teraz adres IP Kaspersky DDoS Protection, który został Ci przydzielony podczas wstępnej konfiguracji. Jednocześnie, ze względu na to, że cyberprzestępcy mogą bezpośrednio zaatakować Twój adres IP, Twój dostawca usług internetowych musi zablokować cały ruch do Twojego pierwotnego adresu IP – z wyjątkiem komunikacji z infrastrukturą Kaspersky DDoS Protection.

Po zmianie Twojego adresu IP cały Twój ruch jest przekierowywany do centrów czyszczenia Kaspersky Lab. „Czysty" ruch jest następnie odsyłany do Twojej firmy za pośrednictwem tuneli wirtualnych GRE.



PO ATAKU

Gdy atak zakończy się, można odblokować pierwotny adres IP i zmienić rekord A serwera DNS – tak aby Twój ruch był ponownie wysyłany bezpośrednio do Twojej firmy.

Sensor Kaspersky Lab nadal gromadzi dane dotyczące Twojego ruchu – i nieustannie przekazuje te dane do naszych serwerów opartych na chmurze, tak abyśmy mogli stale udoskonalać profile zachowania względem typowych warunków, w jakich odbywa się ruch.

Tunele wirtualne pozostają aktywne – wymieniając informacje dotyczące statusu pomiędzy Twoimi routerami oraz routerami firmy Kaspersky lab – tak aby Kaspersky DDoS Protection był gotowy do działania w przypadku, gdy kolejny atak zostanie przeprowadzony na Twoją firmę, a Ty ponownie zdecydujesz się przekierować swój ruch.

Po ataku eksperci z Kaspersky Lab dostarczą również szczegółową analizę oraz raporty określające:

- co stało się podczas ataku,
- jak długo trwał atak,
- w jaki sposób Kaspersky DDoS Protection poradził sobie z atakiem.

INFORMACJE DOTYCZĄCE ZAGROŻEŃ – ZAPEWNIAJĄCE JESZCZE LEPSZĄ OCHRONĘ

Kaspersky DDoS Protection zawiera jeszcze jeden istotny komponent ochrony – komponent, któremu nie mogą dorównać inni producenci

Kaspersky Lab jest pierwszym producentem ochrony antywirusowej, który oferuje rozwiązanie do ochrony przed atakami DDoS – to oznacza, że żaden inny dostawca rozwiązań zapewniających ochronę przed atakami DDoS nie może dorównać doświadczeniu i skali naszego wewnętrznego działu i infrastruktury informacji dotyczących bezpieczeństwa.

W ramach swojej pracy nad rozwojem przełomowej ochrony IT nasi eksperci ds. informacji o zagrożeniach nieustannie monitorują krajobraz zagrożeń w celu identyfikowania nowego szkodliwego oprogramowania i powstających się zagrożeń internetowych. Ci sami eksperci – oraz te same wyrafinowane metody – monitorują również krajobraz zagrożeń DDoS. Dzięki specjalistycznym informacjom możemy wcześniej wykrywać ataki DDoS, dzięki czemu Twoja firma może zostać błyskawicznie objęta ochroną.

WIELOWARSTWOWA OCHRONA

Dzięki niepowtarzalnemu połączeniu ciągłego monitoringu ruchu, analizy statystycznej oraz analizy zachowania – jak również naszym specjalistycznym, proaktywnym informacjom dotyczących ataków DDoS – dostarczamy rozwiązanie zapewniające skuteczną ochronę przed wszelkimi rodzajami ataków DDoS.