Z uwagi na brak dostatecznej liczby chętnych do uruchomienia promocji w 2016 r., niżej opisane warunki świadczenia oraz cennik promocyjny są nieaktualne.

# Jak to działa?

## Natura usługi

### Jakie ataki obsługuje redGuardian, a jakich nie obsługuje?

Obsługuje ataki wolumetryczne UDP, TCP SYN/RST/FIN flood itp. - te zagrażające przepustowości łączy i mechanizmom stanowym.

Czyli odbite NTP, DNS responsy, TFTP data blocki, SSDP UPnP, SNMP… wraz z towarzyszącymi im fragmentami - to wszystko precyzyjnie trafia do śmieci, nawet jeśli ma losowe porty, bo robimy inspekcję w danych pakietu.

Nie mityguje natomiast ataków o małym natężeniu, kierowanych na wyższe warstwy, np. ataków webowych (nie zagląda do TLS/SSL, nie analizuje pod kątem SQL Injection itp.).

| Typ ataku DDoS | Poziom ruchu | Cel | Atakujące adresy IP (liczba/prawdziwość) | Metody neutralizacji |
|---|---|---|---|---|
| wolumetryczny | wiele Gbit/s | wysycenie łączy i całkowite odcięcie | dużo/prawdziwe | scrubbing center, filtry operatorskie |
| stanowy | setki Mbit/s | wysycenie tablic stanowych np. firewalla | dużo/fałszywe (spoofed) | scrubbing center, anti DDoS appliance, zaawansowany firewall i tuning ustawień |
| aplikacyjny | znikomy | wykorzystanie 100% CPU lub pamięci na serwerze aplikacji | średnio/prawdziwe | IPS, cloud-based reverse proxy |
| slow | bliski zera | wysycenie tablic jednocześnie otwartych połączeń na serwerze | niewiele/prawdziwe | tuning i uszczelnianie systemów |

źródło ilustracji: ICT Professional lato 2016

### Jak redGuardian ma się do usługi ochrony webowej z Cloudflare?

To inna, komplementarna usługa.

Cloudflare działa jako odwrotne proxy webowe i skupia się na atakach webowych. Ruch z obydwu kierunkach przechodzi przez ich proxy i ma zmieniany adres IP.

redGuardian działa z kolei jak rozproszony, jednokierunkowy filtr pakietów umieszczony przed Twoją siecią, dzięki czemu może wyciąć ataki wolumetryczne i stanowe zanim zagrożą Twoim łączom i firewallom.

Warto mieć na uwadze, że sprytny atakujący może ustalić prawdziwy adres serwera WWW (nie ten podany w DNS jako adres proxy) i atakować taką sieć bezpośrednio. Dlatego nawet jeśli chronisz swój hosting za Cloudflare, dobrze jest chronić również całą sieć.

## Czy redGuardian swoją ingerencją może popsuć mój ruch?

Platforma wycina kilka rodzajów pakietów obowiązkowo, np. gdy mają złe sumy kontrolne, albo IP z dodanymi IP Options. Tego ruchu raczej i tak nie chcesz obsługiwać.

Pozostałe pakiety są wycinane opcjonalnie, zależnie od reguł, które klient zdecyduje się użyć.

Dla przykładu, filtr na TCP SYN spowoduje kilkusekundową zwłokę podczas otwierania nowego połączenia TCP do usługi hostowanej w Twojej sieci. W przeglądarce widoczne jest to jako “szarpnięcie” podczas pierwszego wejścia na stronę. Jest to skuteczne, ale nie każdy będzie takie zjawisko akceptował.
Z kolei w przypadku fragmentów, niektórzy mogą chcieć wyciąć je całkowicie, a inni przepuszczać je, ale z rate-limitem. W normalnych warunkach fragmenty TCP nie występują, a fragmenty UDP są zjawiskiem rzadkim - mogą nieść np. duże odpowiedzi DNS.

Reasumując, to narzędzie użyte z rozwagą pomoże, a nie zaszkodzi.

## Czy redGuardian wykrywa ataki i reaguje samoczynnie?

Nie, w normalnej sytuacji ruch nie przechodzi przez redGuardiana więc nie ma żadnej wiedzy o tym. Panel webowy posiada REST API, przez które możesz zrobić operacje “On”/”Off” i podpiąć je pod swój automat. Możesz również wysłać do nas pakiet UDP wzywający pomocy. Możesz wreszcie zrobić to ręcznie np. przez smartfona, w reakcji na alarm z Twojego monitoringu.

Kompleksowa automatyzacja jest możliwa np. z wykorzystaniem statystyk SNMP, próbek sFlow/NetFlow lub dedykowanej sondy/sniffera, ale to rozwiązanie ponadstandardowe, dodatkowo płatne.

### Jak zatem mogę rozpoznać, że mam atak?

Sytuacja każdego z podmiotów jest nieco inna. Przykładowe kryteria, które warto śledzić w swoim systemie monitoringu:

- ruch w Mbit/s sięga 100% przepustowości łącza (ale: u niektórych jest to zjawisko normalne w porze szczytu)
- ruch w pps znacznie wzrasta (dość dobre kryterium, ponieważ normalny ruch ma głównie pakiety duże, a atak pakiety małe i średnie)
- udział ruchu UDP w całości ruchu (zwykle znikomy, przy atakach reflected duży)
- udział fragmentów w całości ruchu (zwykle znikomy)
- udział TCP SYN w całości ruchu (zwykle znikomy)
- adresy IP moich next-hopów nie pingują się, adresy IP kluczowych zasobów w Internecie nie pingują się lub mają bardzo wysokie straty

### Jak sterować regułami filtrowania?

Zmiany wprowadza się poprzez webowe GUI. Zmiana jest wdrażana z opóźnieniem około 1 minuty. Możesz przypisać inne reguły do każdego z adresów IP, albo zebrać je w pewne szablony (np. abonenci, hosting, itp.) i zastosować taki szablon dla szerszej podsieci.

Dostarczamy predefiniowany szablon reguł, który w typowych sytuacjach powinien wystarczyć do opanowania ataku.

## BGP i sterowanie ruchem

### Czy ochrona obejmuje wszystkie łącza, czy tylko łącze z EPIX?

Ochrona obejmuje wszystkie łącza, nawet jeśli masz ich np. od 5 dostawców.
Ruch z Internetu, przefiltrowany przez redGuardian, wysyłany jest jednak tylko przez sieć EPIX. Oznacza to, że łącze EPIX powinno być wystarczająco pojemne.

### Mam tylko sieć /24, czy mogę korzystać z tej usługi?

Tak, ale musisz mieć świadomość, że dla /24 nie możemy rozgłosić skutecznie more specific w Internecie. Oznacza to, że ruch przychodzący będzie przekierowany do ochrony tylko częściowo (zależnie od preferencji routerów w Internecie).
Aby zwiększyć skuteczność, możesz jednak przejściowo zaprzestać rozgłaszania swojej sieci /24 do innych operatorów niż EPIX. W ten sposób przerzucisz więcej ruchu na chronioną ścieżkę.

### Czy mogę przekierować do redGuardian tylko jeden adres IP, ten pod atakiem?

Nie - minimalna sieć, która może być przekierowana to /24. Jest to ograniczenie polityk BGP stosowanych powszechnie przez operatorów.

### Czy potrzebne jest zestawienie dodatkowej sesji BGP?

Nie, sterowanie włączeniem/wyłączeniem przekierowania ruchu odbywa się poprzez Web/REST API.

### Czy redGuardian rozgłasza moją sieć pod swoim AS?

Nie, redGuardian będzie widoczny na ścieżce BGP jako jeden z operatorów zagranicznych EPIX Global.Mix. Twoje prefiksy będą widziane nadal pod Twoim AS.

### Czy w razie ataku muszę przekierowywać do redGuardian cały mój ruch przychodzący?

Jeśli masz dokładnie jedną sieć /24 - tak.

Jeśli masz większą pulę adresową, możesz podzielić ją na tzw. prefiksy more specific i przekierować do redGuardian tylko ruch do części sieci. Na przykład, jeśli masz sieć /23, możesz rozgłaszać samodzielnie /23, a w redGuardian rozgłaszać na żądanie te /24 (połówkę), na które idzie atak (do reszty puli adresowej ruch będzie kierowany bez zmian).

## Gdy włączę/wyłączę ochronę, jak szybko ruch będzie przekierowany/oddany?

W praktyce jest to około 1-2 minut w przypadku włączenia.
W przypadku wyłączenia trwa to co najmniej kilka minut, ponieważ trasa do scrubbing center wygasa w światowym BGP stopniowo. Możesz łagodzić to zjawisko:

- przejściowo rozgłaszając równorzędny more specific na swoich łączach chwilę przed wyłączeniem przekierowania,
- redukując w Panelu zasięg przekierowania ruchu z “rozgłaszaj” na “rozgłaszaj tylko w Polsce”, a po kilku minutach (gdy widok z zagranicy się ustabilizuje) wyłączając całkiem (“nie rozgłaszaj”)

Odradzamy szybkie i krótkie włączanie/wyłączanie, aby nie wpaść w BGP dampening oraz nie robić zamieszania w światowej tablicy.

## Czy muszę kłaść w czasie ataku moje sesje BGP?

Jeśli rozgłaszasz przy naszej pomocy prefiksy more specific, to nie.
Jeśli rozgłaszamy prefiksy o tej samej długości (np. masz sieć /24 albo po prostu nie chcesz używać more specificów), rekomendujemy położenie sesji zagranicznych, inaczej ruch trafi do Ciebie częściowo z pominięciem redGuardian. Proces ten da się zautomatyzować na niektórych routerach Cisco/Juniper (warunkowe rozgłaszanie).

## Czy część ruchu “przecieknie” od moich bezpośrednich upstreamów?

Jeśli rozgłosimy more specifics i Twój upstream nie ma magicznych filtrów, to nie - ruch do przekierowanego prefiksu na Twoich uplinkach spadnie do zera (zostanie tylko ruch do reszty prefiksów).

## Czy mogę stosować BGP blackholing?

Tak, możesz używać blackholingu tak jak dotychczas. Jeśli przekierujesz ruch do redGuardian, możesz włączyć blackholing przy pomocy webowego panelu zarządzania. Zastosowania przekierowania z filtrem zamiast blackhola jest przyjaźniejsze dla Twoich klientów, zwłaszcza tych biznesowych.

## Czy muszę uruchamiać dodatkowe łącza, VLAN-y itp.?

Nie.
Ruch do Internetu kierujesz normalnie.
Ruch z Internetu jest “ściągany” z całego świata, w tym od Twoich operatorów.
Ruch z Internetu po przefiltrowaniu trafia do Ciebie istniejącym łączem EPIX.

# Ruch przychodzący z Internetu

## Czy potrzebne jest zestawienie tunelu GRE między moim routerem a redGuardian?

Nie, ruch dosyłany EPIX-em będzie już “odpakowany” z tunelu.

## Czy MTU jest obniżone?

Tak, ruch przychodzący z Internetu, po przefiltrowaniu dotrze tak jakby przeszedł łączem z mniejszym MTU. W normalnych warunkach nie jest to problemem.
Platforma redGuardian wspiera Path MTU Discovery (PMTUD).

Jeśli Państwa router ma taką opcję, rekomendujemy włączenie TCP MSS clamping (MSS adjustment) do 1432B na interfejsach w kierunku wychodzącym do Internetu.

## Jakie dodatkowe opóźnienia w RTT wprowadza przekierowanie ruchu na trasę z ochroną?

Jeśli chodzi o aspekt sieciowy, w realiach Polski są to opóźnienia znikome, liczone w pojedynczych milisekundach. Na niektórych trasach zagranicznych może się okazać, że opóźnienia różnią się np. o 10ms (mniej lub więcej), co wyniknie po prostu z kierowania innymi operatorami niż normalnie.
Jeśli chodzi o samą platformę, nie wprowadza ona opóźnień większych niż switch, bo nie kolejkuje ruchu.

## Co gdy mam dwa łącza do EPIX, w Warszawie i Katowicach?

Ruch przefiltrowany będzie wrzucany do szkieletu EPIX i może trafić mniej więcej po połowie na te dwa węzły. Dokładnie rozwiązanie zostanie wypracowane na etapie pilota.

# Ruch wychodzący do Internetu

## Jak redGuardian wpływa na kierowanie ruchu wychodzącego z mojej sieci?

Ruch wychodzący do Internetu może być kierowany bez zmian.
Ruch przychodzący z Internetu będzie “ściągany” do scrubbing center redGuardian, a następnie dosyłany do EPIX i dalej do Państwa sieci.
Taka asymetria ruchu nie stanowi problemu w Internecie.

### Czy muszę jakoś modyfikować ruch wychodzący?

Rekomendujemy użycie TCP MSS Clamping/Adjustment w celu redukcji TCP MSS z 1460B do 1432B na wszystkich łączach wyjściowych. Nie jest to niezbędne, ale pomoże w sytuacjach, gdy PMTUD zawodzi.

## RIPE

### Czy potrzebne są zmiany w RIPE whoisdb?

Może być konieczne dodanie obiektów “route” dla tras more specific, które będą rozgłaszane warunkowo przez redGuardian. Na etapie setupu usługi doradzimy, czy i co tutaj dodać.

# Promocja z EPIX

### Jaki jest plan działań?

- Zbieramy zapisy, budujemy księgę popytu. ;-)
- Jeśli widzimy skalę, która da niską cenę per podmiot, odpalamy pilotaż.
- Po pilocie zbieramy wnioski, poprawiamy i przechodzimy w tryb produkcyjny.

### Co będzie, jeśli nie nazbiera się wystarczająca liczba chętnych?

Wówczas promocja o tak niskiej cenie nie będzie możliwa.

Przy bardzo dużej liczbie klientów zaczyna to działać jak składka ubezpieczeniowa, jest dość niska i od czasu do czasu każdy może skorzystać, gdy ma pecha i staje się celem ataku. Tylko duża liczba małych składek pozwala na utrzymanie tak zaawansowanej infrastruktury.

### Jakie są ograniczenia promocyjnej oferty dla EPIX?

- tylko mali i średni ISP, na własne potrzeby
- dosył ruchu po przefiltrowaniu tylko przez EPIX
- do 2Gbit/s dla ruchu czystego (powiększenie za dopłatą)
- do 72h wykorzystania w skali miesiąca (powiększenie za dopłatą)
- model abonamentowy i długofalowa współpraca (brak możliwości zakupu “od teraz, na miesiąc”)
- podstawowe wsparcie

### Czy mogę odebrać ruch przefiltrowany wszystkimi moimi łączami, a nie tylko EPIX?

Technicznie - tak, ale jest to wyraźnie droższa oferta komercyjna, a nie promocyjna.

### Czy mogę mieć włączoną ochronę przez cały czas?

Promocyjna oferta nakłada limit wykorzystania 72h w miesiącu.
Po przekierowanie ruchu powinniśmy zatem sięgać tylko wtedy, gdy mamy atak (on demand).
Uruchomienie na stałe (always on) wymaga indywidualnej wyceny.

## Gdzie mogę poczytać coś więcej nt. tego rozwiązania?

- https://www.redguardian.eu/pl/dzialanie-systemu
- http://www.slideshare.net/atendesoftware/redguardian-antyddos-dla-epix-kike-xviii
- https://youtu.be/1E4BwIvDjjI?t=16303
- http://www.slideshare.net/atendesoftware/redguardian-antyddos