NASK SA
secure and safe data

NASK SA Cyber Security

DDoS Attack Protection

NASK SA
ul. Wąwozowa 18 lok. 010, 02-796 Warszawa
tel.: +48 22 182 00 00, fax: +48 22 182 00 10
kontakt@nasksa.pl, www.nasksa.pl
NIP: 9512421815, REGON: 365743505

Bank: Raiffeisen Bank Polska S.A.
Numer konta: 68 1750 0009 0000 0000 3492 1587
Kapitał zakładowy w wysokości 41.100.000 zł (czterdzieści jeden milionów sto tysięcy złotych) wpłacony w całości
S.R. dla m.st. Warszawy XIII Wydział Gospodarczy KRS, nr KRS 0000644422

NASK SA w ramach grupy usług **NASK SA Cyber Security** oferuje usługę **DDoS Attack Protection** (ang. DDoS – *Distributed Denial of Service*) chroniącą przed skutkami rozległych ataków wolumetrycznych, przeprowadzanych równocześnie z wielu komputerów. Ataki DDoS polegają na uniemożliwieniu działania systemu komputerowego lub usługi sieciowej przez zajęcie wszystkich wolnych zasobów. Nie radzą sobie z nimi klasyczne systemy bezpieczeństwa jak NGFW czy IPS, które nie rozróżniają ataku od ruchu legalnego. Dlatego korzystne jest zastosowanie specjalistycznych mechanizmów operatorskich zaimplementowanych możliwe jak najdalej od punktu styku z sieci LAN klienta z Internetem.

Oferowana przez NASK SA usługa ochrony przed atakami DDoS polega na filtrowaniu na stykach sieci NASK SA niepożądanego ruchu noszącego znamiona ataku DDoS. Oferowana w dwóch wariantach, Standard i Premium, jest skierowana jest do klientów dysponujących łączem zestawionym przez NASK SA.

Istotne definicje:

- mitygacja, czyli czyszczenie ruchu – proces minimalizowania niepożądanego ruchu IP noszącego znamiona ataku DDoS, w sposób możliwie najmniej ograniczający oczekiwany ruch IP kierowany do klienta;
- filtracja ruchu – proces ograniczania niepożądanego ruchu IP noszącego znamiona ataku DDoS;
- obiekt (ang. *Managed Object*) - pojedynczy adres IP, lub zakres adresacji IP objęty usługą **DDoS Attack Protection**;
- pojedynczy atak DDoS – atak DDoS trwający do 24 godzin;
- długotrwały atak DDoS - atak DoS/DDoS trwający powyżej 24 godzin;
- Learning Mitigation – proces nauki polegający na analizie ruchu IP klienta w celu identyfikacji odchyleń od oczekiwanego ruchu IP przychodzącego do chronionych obiektów klienta.

NASK SA
secure and safe data

Porównanie wariantów usługi DDoS Attack Protection

	DDoS Attack Protection Standard	DDoS Attack Protection Premium
Mechanizmy wykorzystywane do monitorowania	System monitorowania przepływów w sieci na bazie protokołu NetFlow.	1. System monitorowania przepływów w sieci na bazie protokołu NetFlow. 2. Dedykowany system monitorowania chronionych obiektów Peak Flow Arbor Networks zaimplementowany przy routerach sieci szkieletowej NASK SA.
Mechanizmy mitygacji ataków	1. BGP Blackholing dla blokowania ruchu z/do określonej podsieci IP. 2. BGP FlowSpec wykorzystywany do dystrybucji list kontrolnych ACL za pomocą protokołu MP-BGP	1. Dedykowany system do mitygacji ataków TMS Arbor Networks. 2. BGP FlowSpec wykorzystywany do dystrybucji list kontrolnych ACL za pomocą protokołu MP-BGP. 3. BGP Blackholing dla blokowania ruchu z/do określonej podsieci IP.
Opis mechanizmów mitygacyjnych	Mechanizmy mitygacyjne pozwalają na zablokowanie ruchu z/do określonej podsieci IP i/lub filtracje niepożądanego ruchu charakteryzującego się następującymi parametrami: • adres IP źródłowy i docelowy, • wykorzystywany port, protokół, pole w datagramie IP – DSCP, • flagi w protokole TCP.	Mechanizm ten pozwala na bardzo selektywną mitygację ruchu w ramach autorskich algorytmów zaimplementowanych w systemie Arbor Networks. Do selektywnej mitygacji niepożądanego ruchu usługa wykorzystuje zewnętrzne, światowe bazy reputacyjne, prowadzone przez firmę Arbor Networks. Dodatkowo system koreluje ruch przychodzący do klienta w trakcie ataku z ruchem będącym normalnym trybem pracy. Przy atakach DDoS nie przekraczających 5 Gbps wykorzystywany jest w pełni system do selektywnej mitygacji ataku – Arbor Networks. W przypadku gdy atak przekracza wartość 5 Gbps operatorzy NASK w porozumieniu z klientem wykorzystają w pierwszym etapie mechanizmy zgrubnej filtracji wariantu Standard ograniczając go do poziomu < 5 Gbps, tak aby system Arbor przeprowadził selektywną mitygację.
Gwarantowana Mitygacja ataku	-----	do 5 Gbps
Czas działania Mitygacji	do 72 godz.	do 72 godz.
Standardowa liczba chronionych Obiektów - prefixów IP	5	5

Proaktywny monitoring 24h	tak	tak
Nieograniczona Mitygacja ataków	tak	tak
Raport po ataku	nie	tak
Gwarancje jakości usługi		
Dostępność usługi (w okresie rozliczeniowym)	99,5%	99,5%
Czas reakcji na atak	Czas Reakcji na atak to czas pomiędzy wykryciem ataku zarejestrowanym w wewnętrznym systemie monitorowania sieci NASK SA, a skutecznym zakończeniem procedury informowania abonenta przez operatorów NOC/SOC.	
	15 min.	15 min.
Czas uruchomienia mitygacji	Czas gwarancji uruchomienia mitygacji to czas pomiędzy skutecznym poinformowaniem abonenta i otrzymaniem akceptacji na uruchomienie procesu mitygacji, do momentu jej uruchomienia przez NASK SA.	
	30 min.	15 min.

NASK SA
ul. Wąwozowa 18 lok. 010, 02-796 Warszawa
tel.: +48 22 182 00 00, fax: +48 22 182 00 10
kontakt@nasksa.pl, www.nasksa.pl
NIP: 9512421815, REGON: 365743505

Bank: Raiffeisen Bank Polska S.A.
Numer konta: 68 1750 0009 0000 0000 3492 1587
Kapitał zakładowy w wysokości 41.100.000 zł (czterdzieści jeden milionów sto tysięcy złotych) wpłacony w całości
S.R. dla m.st. Warszawy XIII Wydział Gospodarczy KRS, nr KRS 0000644422