

## Jak zablokować P2P w 1 minutę?

Prawdziwym problemem dla firm są programy typu peer-to-peer, służące do pobierania plików z Internetu, używane przez pracowników na firmowych komputerach. Po pierwsze w znaczący sposób obciążają firmowe łącza, co pływa na wydajność pracy w sieci. Po drugie, programy P2P umożliwiają pobierania z Internetu niedozwolonych przez polskie prawo treści takich jak filmy, pliki muzyczne czy nielegalne wersje oprogramowania. Aprobata dla takiego procederu skutkować może poważnymi konsekwencjami karnymi dla firmy. Po trzecie to często źródło złośliwego oprogramowania takiego jak wirusy czy Trojany.

Autorzy aplikacji P2P tworzą nowe, zaawansowane sposoby obejścia blokad na firewallu. Do ich blokowania posłużyć się należy rozwiązaniami z funkcją IDS/IPS, która analizuje sygnatury połączenia i dzięki temu daje administratorom możliwość blokowania ruchu P2P przechodzącego przez firewall.

Jednym z dostępnych na rynku zintegrowanych rozwiązań jest urządzenie NETASQ UTM, z wbudowanym w nie autorskim modułem IPS. IPS posiada bazę sygnatur niechcianego przez administratorów ruchu. Jego konfigurowanie odbywa się w nieskomplikowany sposób z użyciem konsoli graficznej Administration Suite. Poniżej zobaczyć można jak uruchomić blokowanie w minutę.

### Monitoring i zarządzanie

Potrzebne do tego będą 2 narzędzia wchodzące w skład aplikacji NETASQ Administration Suite: NETASQ Unified Manger i NETASQ Real-Time Monitor. NETASQ Unified Manager służy na konfigurowania urządzenia, a NETASQ Real-Time Monitor pozwala śledzić aktywności użytkowników w czasie rzeczywistym.

Przed zablokowaniem aplikacji możesz za pomocą NETASQ Real-Time Monitora sprawdzić, na których stacjach roboczych generowany jest uciążliwy ruch. Opisałem to w części *Wykrywanie ruchu*. Jeśli zamierzasz od razu przejść do instrukcji *Blokowanie ruchu* pomiń pierwszą część.

### Wykrywanie ruchu

Najpierw sprawdź jaki ruch jest generowany na komputerach użytkowników sieci za pomocą programu NETASQ Real-Time Monitor, która pozwoli Ci przeglądać alarmy IPS w czasie rzeczywistym. Po otwarciu aplikacji **NETASQ Real-Time Monitor** przejdź do sekcji **Alarms**.

Date	Sensible	Copy	Priority	Rule	Action	Interface	Protocol	Source	Destination	Destination port	Message	Packet
13:23:45	4	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:23:39	0	0	Minor	0	pass	In	http	hp	www-google-analytics.l.google.com	http	Misc : Remote code execution prevention: 2   characters fo...	
13:23:39	0	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:23:02	No	0	Minor	0	pass	In	icmp	hp	Firewall_out_dns1	hp	Allowed by ICMP analyze	
13:23:00	0	0	Minor	0	pass	In	http	hp	74.125.39.113	http	Misc : Remote code execution prevention: 2   characters fo...	
13:23:00	0	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:23:00	2	0	Minor	0	pass	In	http	hp	74.125.39.113	http	Misc : Remote code execution prevention: 2   characters fo...	
13:22:39	0	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:22:39	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:39	No	2	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:35	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:35	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:31	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:31	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:26	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:26	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet	
13:22:21	0	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:22:21	0	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http	Multimedia : Flash/shockwave content detected	
13:21:13	0	0	Minor	0	block	Out	http	hp	s2.hk.sta24.com	http	Multimedia : Flash/shockwave content detected	
13:20:35	No	0	Minor	0	pass	In	http	hp	tracker.openbittorrent.com	http	Bad UTF-8 encoding in URL	
13:20:35	0	0	Minor	0	pass	In	http	hp	tracker.openbittorrent.com	http	P2P : BitTorrent announces	
13:20:34	No	0	Minor	0	block	In	http	hp	torrentbay.pl	http	Wrong TCP sequence number (fast duplicate ACK)	
13:20:34	No	5	Minor	0	block	In	http	hp	torrentbay.pl	http	Wrong TCP sequence number (fast duplicate ACK)	
13:20:33	0	0	Minor	0	block	Out	http	hp	dc.sabela.pl	http	Multimedia : Flash/shockwave content detected	
13:20:32	No	0	Minor	0	block	Out	http	hp	img251.imageshack.us	http	Wrong TCP sequence number (closed window)	
13:20:32	No	0	Minor	0	block	Out	http	hp	img19.imageshack.us	http	Wrong TCP sequence number (closed window)	
13:20:32	No	3	Minor	0	block	Out	http	hp	img19.imageshack.us	http	Wrong TCP sequence number (closed window)	
13:20:32	No	5	Minor	0	block	Out	http	hp	img251.imageshack.us	http	Wrong TCP sequence number (closed window)	
13:20:10	No	0	Minor	0	pass	In	http	hp	85.17.80.246	http	Bad UTF-8 encoding in URL	

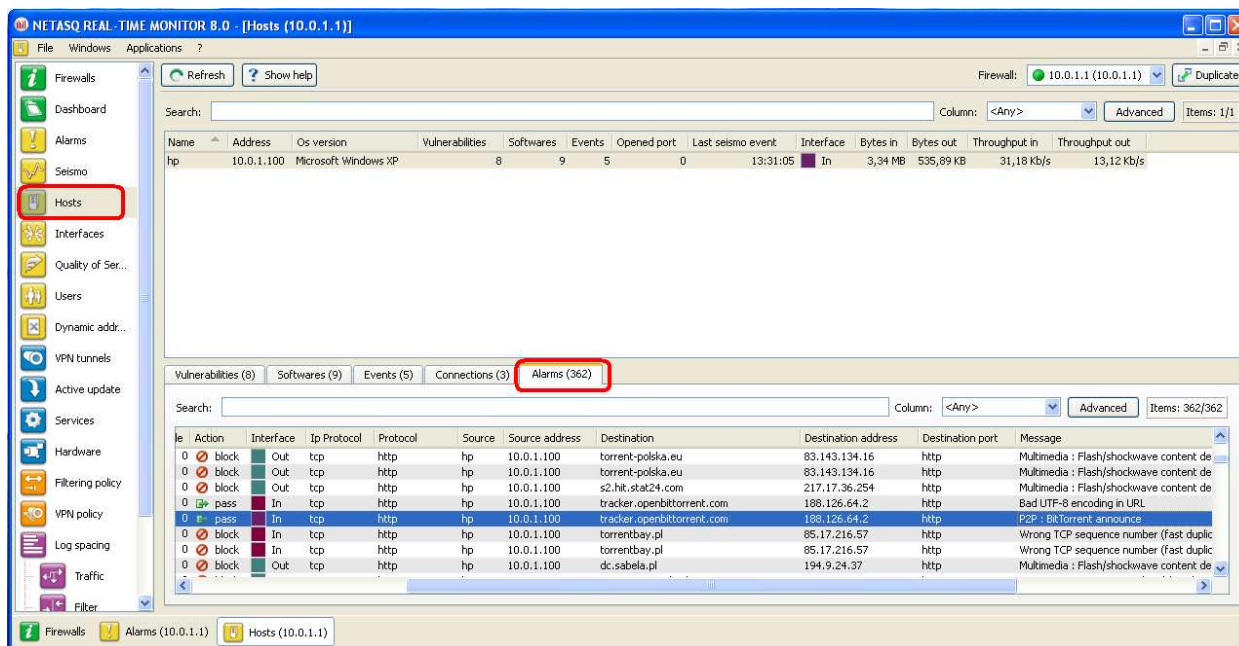
W sekcji **Alarms** wyświetlona zostanie lista wszystkich alarmów IPS, które możesz sortować w dowolny sposób np. chronologicznie (**Date**), według protokołu (**Protocol**), źródła (**Source**) lub sygnatury alarmu (**Message**).

W ten sposób odszukaj na liście nazwę odpowiedniej sygnatury ruchu. Źródło niechcianej aktywności wyświetlane w kolumnie **Source** może podawać nazwę lub adresy IP stacji roboczych, których ten ruch dotyczy.

Tutaj ruch „**P2P : BitTorrent announce**” z hosta o nazwie „**hp**”.

Date	Sensible	Copy	Priority	Rule	Action	Interface	Protocol	Source	Destination	Destination port	Message	Packet
13:22:21	0	Minor	0	block	Out	http	hp	torrent-polska.eu	http		Multimedia : Flash/shockwave content detected	
13:22:21	5	Minor	0	block	Out	http	hp	torrent-polska.eu	http		Multimedia : Flash/shockwave content detected	
13:21:13	0	Minor	0	block	Out	http	hp	s2.hit.stat24.com	http		Multimedia : Flash/shockwave content detected	
13:20:35	No	0	Minor	0	pass	In	http	hp	tracker.openbittorrent.com	http	Bad UTF-8 encoding in URL	
13:20:35	0	Minor	0	pass	In	http	hp	tracker.openbittorrent.com	http		<b>P2P : BitTorrent announce</b>	
13:20:34	No	0	Minor	0	block	In	http	torrentbay.pl	http		wrong TCP sequence number (fast duplicate ACK)	

Innym sposobem jest wyszukiwanie sygnatur ruchu za pomocą sekcji **Hosts**, która w zakładce **Alarms** wyświetla informacje o alarmach na wskazanej stacji roboczej. Poniżej lista alarmów dla hosta „hp”.

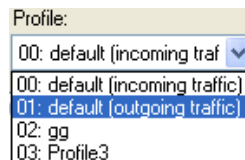


Na wykazie alarmów dla stacji „hp” odszukaj nazwy sygnatury.

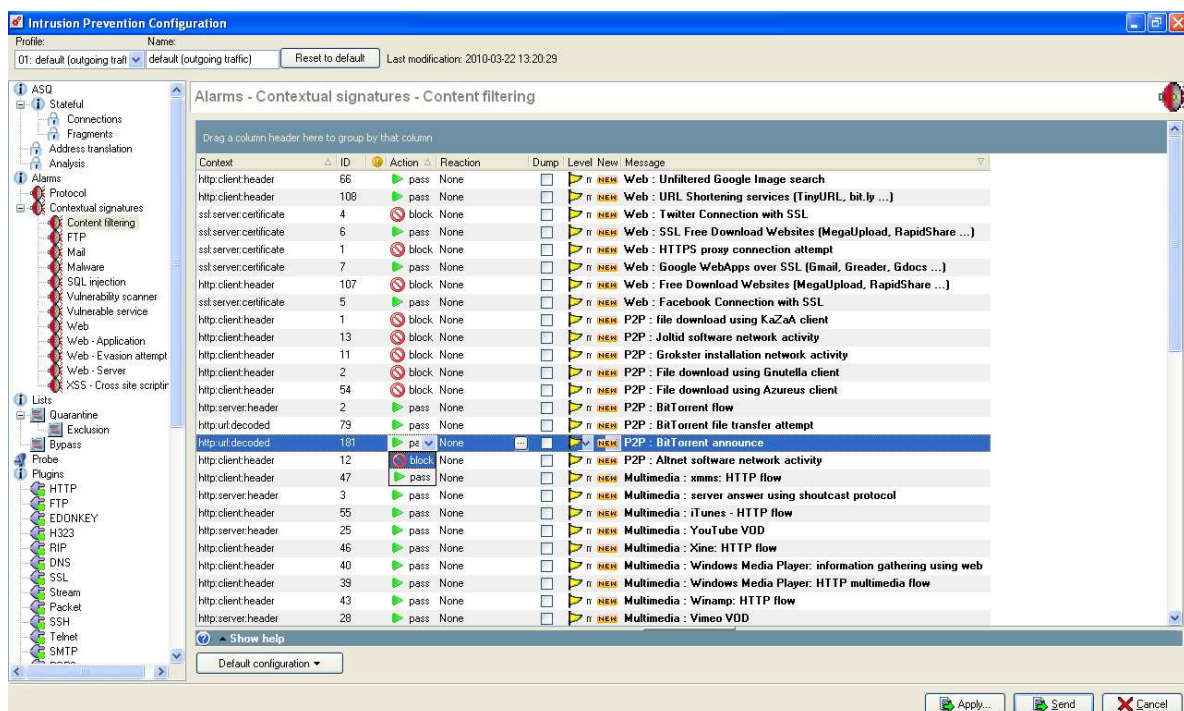
Action	Interface	Ip Protocol	Protocol	Source	Source address	Destination	Destination address	Destination port	Message
block	Out	tcp	http	hp	10.0.1.100	torrent-polska.eu	83.143.134.16	http	Multimedia : Flash/shockwave content de
block	Out	tcp	http	hp	10.0.1.100	torrent-polska.eu	83.143.134.16	http	Multimedia : Flash/shockwave content de
block	Out	tcp	http	hp	10.0.1.100	s2.hit.stat24.com	217.17.36.254	http	Multimedia : Flash/shockwave content de
pass	In	tcp	http	hp	10.0.1.100	tracker.openbittorrent.com	188.126.64.2	http	Bad UTF-8 encoding in URL
pass	In	tcp	http	hp	10.0.1.100	tracker.openbittorrent.com	188.126.64.2	http	<b>P2P : BitTorrent announce</b>
block	In	tcp	http	hp	10.0.1.100	torrentbay.pl	85.17.216.57	http	wrong TCP sequence number (fast duplic
block	In	tcp	http	hp	10.0.1.100	torrentbay.pl	85.17.216.57	http	Wrong TCP sequence number (fast duplic
block	In	tcp	http	hp	10.0.1.100	dc.sabela.pl	194.9.24.37	http	Multimedia : Flash/shockwave content de

## Blokowanie ruchu

Skoro znasz już nazwy sygnatur ruchu uruchom program NETASQ Unified Manager. Zwróć uwagę, aby pole **Profile** w lewym nagłówku ustawione było na „**01: default (outgoing traffic)**”.



W aplikacji NETASQ Unified Manager po wybraniu sekcji **Intrusion Prevention** przejdź do konfigurowania modułu IPS, który wyświetli się w nowym oknie. W lewej tabeli dostępne będzie menu. Wskaż w nim **Contextual signatures** → **Content filtering**.



W kolumnie **Message** w głównym oknie wyświetlają się sygnatury ruchu. Wybierz tą, którą chcesz zablokować. Blokowanie odbywa się poprzez zaznaczenie sygnatury oraz wybranie w kolumnie **Action** polecenia **Block**.

Aby zapisać i aktywować wprowadzone zmiany kliknij w pole  w prawym dolnym rogu okna. Od tego momentu ruch „**P2P : BitTorrent announce**” będzie blokowany przez system IPS.