

## Jak zablokować komunikatory internetowe na przykładzie Gadu-Gadu?

Pracownicy, którzy na swoich komputerach firmowych korzystają z aplikacji sieciowych, mogą narażać na niebezpieczeństwo zainfekowania szkodliwymi zawartościami lokalną sieć. Dotyczy to również używania komunikatorów internetowych (Gadu-Gadu, Tlen), które mogą być źródłem zagrożeń. Niektórzy administratorzy nie kontrolują jakie programy sieciowe instalują użytkownicy na firmowych komputerach. Wtedy pomocne mogą stać się rozwiązania pozwalające na monitorowanie połączeń i - co bardziej przydatne - blokowanie tych, potencjalnie niebezpiecznych.

Takie funkcje posiada urządzenie NETASQ UTM - firewall z wbudowanym modulem IPS i kilkoma funkcjonalnościami podnoszącymi poziom bezpieczeństwa sieci (VPN, ochrona anytwirusowa, ochrona antyspamowa, filtr URL i autoryzacja). System blokowania włamań IPS dokładnie skanuje cały ruch w sieci. Dzięki analizowaniu ruchu w warstwach od 3 do 7 (modelu ISO/OSI), NETASQ potrafi wykrywać aplikacje korzystające z połączenia z Internetem.

Administrowanie urządzeniem NETASQ z poziomu Windows odbywa się za pomocą pakietu aplikacji Administration Suite. W jej skład wchodzi programy NETASQ Unified Manager, Real-Time Monitor oraz Event Reporter. Pierwszy z nich służy do zarządzania i administrowania urządzeniem. Drugi pozwala monitorować pracę urządzenia w czasie rzeczywistym. Trzecie narzędzie umożliwia przeglądanie dziennika zdarzeń.

Dzięki NETASQ administrator może sprawdzać z jakich aplikacji sieciowych korzystają pracownicy a następnie je zablokować. Jak to zrobić w prosty sposób zaprezentowano poniżej na przykładzie polskiego komunikatora Gadu-Gadu.

### Monitorowanie połączeń

Za pomocą dostarczonej bezpłatnie przez producenta aplikacji NETASQ Real-Time Monitor możesz monitorować aktywność aplikacji sieciowych w czasie rzeczywistym. Pozwala ona sprawdzić m.in. czy użytkownicy korzystają z komunikatorów internetowych i innych niechcianych programów. Możesz zablokować wybrany rodzaj połączeń bez sprawdzania czy pracownicy z nich korzystają.

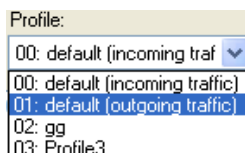
Uruchom program Real-Time Monitor, żeby sprawdzić, co robią użytkownicy w sieci. W lewym menu wskaż sekcję **Alarms**. W głównym oknie wyświetli się lista komunikatów generowanych przez system wykrywania i blokowania włamań IPS, który analizuje przychodzące i wychodzące połączenia.

Date	Sensible	Copy	Priority	Rule	Action	Interface	Protocol	Source	Destination	Destination port	Message
14:24:40	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:24:39	No	0	Minor	0	pass	In	http	hp	m.d.onet.pl	http	Multiple slash in URL
14:24:39	No	0	Minor	0	block	Out	http	hp	wiadomosci.onet.pl	http	Multimedia : Flash/shockwave content detected
14:24:38	No	0	Minor	0	block	Out	http	hp	reklama.d.onet.pl	http	Multimedia : Flash/shockwave content detected
14:24:37	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:24:32	No	0	Minor	0	block	Out	http	hp	reklama.d.onet.pl	http	Multimedia : Flash/shockwave content detected
14:24:32	No	3	Minor	0	block	Out	http	hp	reklama.d.onet.pl	http	Multimedia : Flash/shockwave content detected
14:24:16	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:23:55	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:23:55	No	0	Minor	0	pass	Out	https	hp	GG_servery	https	IM : Gadu-Gadu Messenger client (SSL)
14:23:55	No	2	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:23:34	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet
14:23:34	No	2	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet
14:23:17	No	0	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet
14:23:17	No	2	Minor	0	pass	In	netbios-dgm	hp	10.0.1.255	netbios-dgm	Broadcast packet
14:22:38	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:22:35	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:22:14	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:21:52	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:21:52	No	0	Minor	0	pass	Out	https	hp	GG_servery	https	IM : Gadu-Gadu Messenger client (SSL)
14:21:52	No	2	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:21:31	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:21:28	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:21:07	No	0	Minor	0	block	In	8074	hp	GG_servery	8074	Invalid TCP packet for current connection state (CLIE...
14:20:46	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:20:46	No	0	Minor	0	pass	Out	https	hp	GG_servery	https	IM : Gadu-Gadu Messenger client (SSL)
14:20:46	No	2	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:20:38	No	0	Minor	0	block	In	8074	hp	gpproxy-1.gadu-gadu.pl	8074	Invalid TCP packet for current connection state (CLIE...
14:20:35	No	0	Minor	0	block	In	8074	hp	gpproxy-1.gadu-gadu.pl	8074	Invalid TCP packet for current connection state (CLIE...
14:20:14	No	0	Minor	0	block	In	8074	hp	gpproxy-1.gadu-gadu.pl	8074	Invalid TCP packet for current connection state (CLIE...
14:20:11	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:20:11	No	2	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:19:58	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:19:58	No	4	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client
14:19:53	No	0	Minor	0	pass	In	http	hp	apmsg.gadu-gadu.pl	http	IM : Gadu-Gadu Messenger client

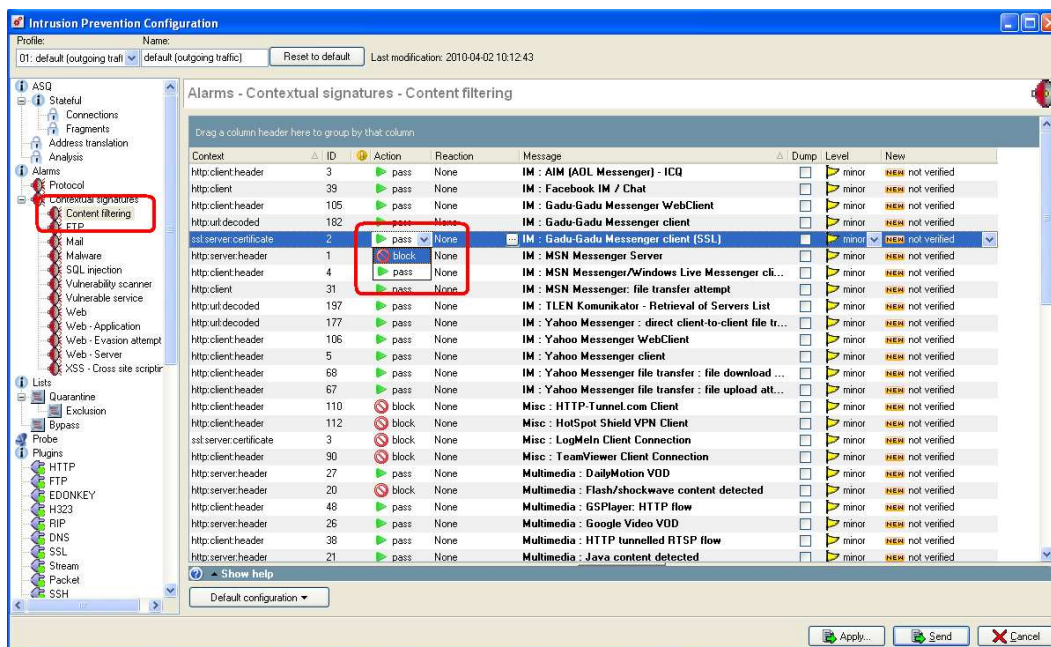
Masz pełną dowolność w sortowaniu pojawiających się na bieżąco alarmów np. według źródeł (**Source**), protokołów (**Protocol**) lub adresu docelowego (**Destination**). Na liście sygnatur (**Message**) można odnaleźć sygnatury ruchu według ich nazw. W powyższym przykładzie zaznaczone są sygnatury połączenia **IM: GaduGadu Messenger client (SSL)**.

### Blokowanie komunikatora

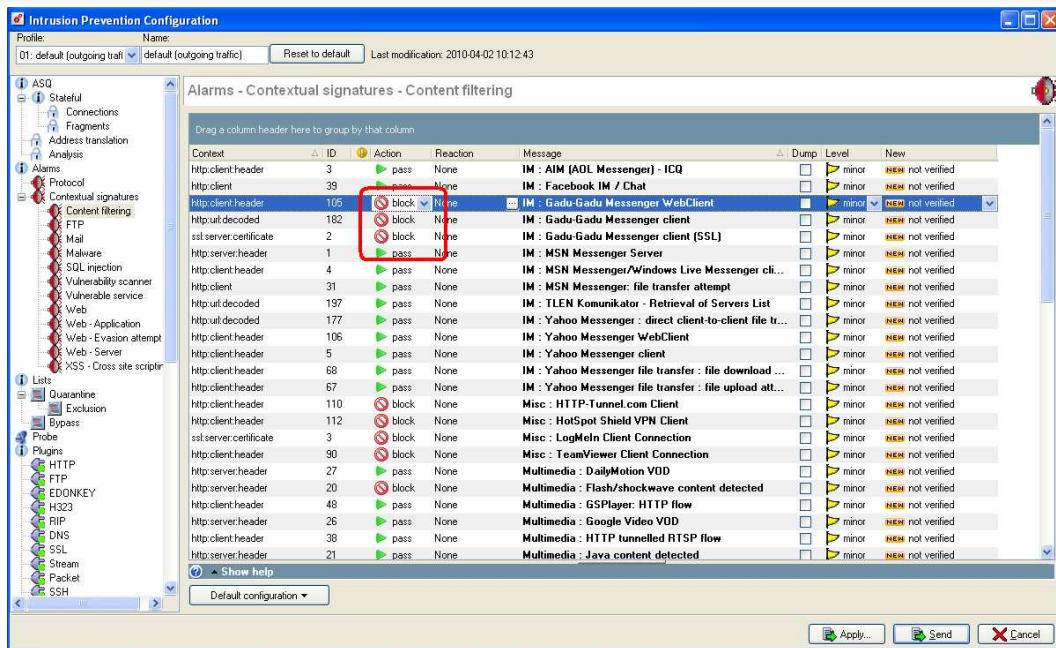
Wróć do konsoli NETASQ Unified Manager. Wybierz sekcję **Intrusion Prevention**. Jej zawartość powinna wyświetlić się w nowym oknie. Przejdź do konfigurowania. Zauważ czy pole **Profile** w lewym nagłówku ustawione jest na „**01: default (outgoing traffic)**” (dla urządzeń serii „U” czyli np. U30, U70, itd). Ustaw poprawnie profil.




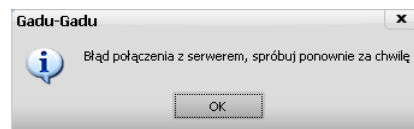
W lewym menu wybierz **Contextual signatures** → **Content filtering**.



W kolumnie **Message** w głównym oknie wyświetlane są sygnatury ruchu. Możesz agregować je w dowolny sposób przeciągając na szary pasek. Wybierz i zaznacz te z nich, które chcesz zablokować. W kolumnie **Action** ustaw polecenie akcji na **Block**. Możesz zablokować dowolne typy komunikatorów jak Gadu-Gadu, Tlen czy Messenger.



Następnie, aby zapisać i uruchomić wprowadzone zmiany kliknij w pole  w prawym dolnym rogu okna. Od tego momentu każde kolejne próby połączenia się użytkownikami z serwerem Gadu-Gadu będą niemożliwe, a użytkownicy zobaczą następujący komunikat.



Jeśli chcesz zablokować pozostałe aplikacje komunikatorów internetowych, zastosuj powyżej opisaną instrukcję.