

ZALECENIA DLA MIGRACJI NS-BSD V8 => V9

Wprowadzenie

Wersja 9 NS-BSD wprowadza wiele zmian. Zmieniła się koncepcja działania niektórych modułów NETASQ UTM. Sam proces aktualizacji nie jest więc całkowicie automatyczny. Celem niniejszego dokumentu jest opisanie kolejnych czynności, które powinny zostać wykonane przed i po aktualizacji firmware'u z wersji 8 do 9.

Zarządzanie w wersji 9

Główną zmianą w nowej wersji firmware'u NETASQ jest konsola zarządzająca. Od wersji 9 administracja NETASQ odbywa się bowiem przy użyciu konsoli WEB. Konfiguracja za pośrednictwem przeglądarki zastąpi aplikację *Unified Manager*. Poniższa tabela przedstawia listę aplikacji dla obu wersji NS-BSD.

	Firmware wersja 8	Firmware wersja 9
Konfiguracja	Unified Manager 8	Konsola WEB
Monitoring	Real Time Monitor 8	Real Time Monitor 9
Przeglądanie logów	Event Reporter 8	Event Reporter 9
Raporty	Event Reporter 8	Event Analyzer 1.0

W obu wersjach systemu administrator ma dostęp do wiersza poleceń CLI, przy wykorzystaniu protokołu SSH lub podłączając się bezpośrednio do portów VGA lub COM.

Wspierane platformy

Aktualizacja do wersji NS-BSD 9 jest możliwa tylko dla urządzeń serii U oraz NG. Najstarsza wersja firmware'u, dla której można przeprowadzić aktualizację to **NS-BSD 8.0.3**.

Wspierane przez konsolę WEB przeglądarki internetowe to:

- Microsoft Internet Explorer 7 i 8
- Firefox 3.6 lub nowszy

Internet Explorer w wersji 9 zostanie dodany do obsługiwanych przeglądarek w chwili, gdy wersja ta stanie się wersją finalną.

Wersja 9 pakietu zarządzającego (**Administration Suite**) jest kompatybilna z systemami operacyjnymi:

- Microsoft Windows XP, Vista, 7
- Microsoft Windows Server 2003, Server 2008, Server 2008 R2

Oprogramowanie Administration Suite można pobrać z NETASQ Client Area lub za pośrednictwem:

www.dagma.pl/new/netasq/software/as_9.exe

UWAGA

Wsparcie techniczne, aktualizacje firmware'u i sygnatur pozostają aktywne dla wersji 8.

Proces aktualizacji

Aktualizacja w środowisku produkcyjnym

Aktualizacja firmware'u nie jest całkowicie automatyczna i powoduje przywrócenie niektórych modułów i funkcji UTM do ustawień fabrycznych (szczegółowy wykaz zmian na końcu niniejszego dokumentu). W związku z tym aktualizacja zdalna nie jest zalecana.

W celu skrócenia przerwy w dostępie do sieci firmowej, związanej z konfiguracją urządzenia NETASQ, administrator może wykonać konfigurację na przygotowanej przez producenta maszynie wirtualnej, a następnie przenieść gotową konfigurację do urządzenia produkcyjnego.

Obraz firmware'u 9 (w postaci maszyny wirtualnej) oraz niezbędna licencję będzie można pobrać z sekcji „Private area” na stronie www.netasq.com, po wydaniu finalnej wersji firmware'u 9.

Przed rozpoczęciem aktualizacji firmware'u do wersji 9 zalecamy wykonanie backupu wersji 8 na zapasowej partycji oraz wykonanie kopii zapasowej konfiguracji do pliku (full backup). W każdej chwili po zakończonej aktualizacji firmware'u do najnowszej wersji można ponownie uruchomić urządzenie oraz system z partycji zapasowej. Można wtedy także wykonać kopię partycji (z zapasowej na główną) co spowoduje, iż obie partycje będą w wersji 8.

Klaster wysokiej dostępności (High Availability)

Podczas aktualizacji do wersji 9, urządzenie pracujące w klastrze nie jest odłączane. W rezultacie obydwie urządzenia pracują jednocześnie w trybie aktywnym, stąd konieczność rozłączenia obu urządzeń na czas wgrzywania nowego firmware'u.

Dostęp administracyjny po wykonaniu aktualizacji

Dostęp do urządzenia po pomyślnej aktualizacji będzie możliwy jedynie z komputerów w tej samej adresacji co wewnętrzne interfejsy NETASQ.

Sygnatury

Po wykonaniu aktualizacji NS-BSD zalecamy wykonanie pełnej aktualizacji sygnatur (IPS/AV/Antyspam/SEISMO/URL), którą można wykonać z poziomu CLI poleceniem:

```
`autoupdate -f`
```

Nowości w wersji 9

Sekcja przedstawia zmiany koncepcyjne w konfiguracji urządzenia z którymi należy zapoznać się przed wykonaniem migracji NS-BSD do najnowszej wersji.

Zarządzanie z poziomu przeglądarki internetowej

Urządzenia NETASQ od firmware'u w wersji 9 posiadają konsolę zarządzającą WEB, zastępującą dotychczasową aplikację NETASQ Unified Manager, która umożliwia konfigurowanie rozwiązań NETASQ z poziomu przeglądarki Internetowej.

Po wykonaniu aktualizacji do wersji 9 interfejs zarządzający jest dostępny na porcie 443 (https).

Administrator może podłączyć się do urządzenia wpisując w przeglądarkę adres:

https://IP_urządzenia_Netasq/admin/

użytkownik: admin, hasło: zdefiniowane przez administratora.

Port 443 może zostać zmieniony po podłączeniu się do urządzenia: *System -> Configuration -> w zakładce Firewall administration*

W ten sam sposób administrator może określić z jakich hostów/podsieci będzie można zarządzać urządzeniem UTM.

Dodatkowo w sekcji *System -> Administration -> User Priviledge* administrator może określić jaki poziom uprawnień będzie miała osoba w chwili podłączenia się do urządzenia w celu jego zarządzania.

Uwaga!

Jeżeli w konfiguracji translacji adresów NAT będzie potrzeba przekierowania portu https (domyślny port dla administracji urządzeniem NETASQ) to należy przed ustawieniem przekierowania zmienić domyślny port administracyjny. W przeciwnym wypadku może nastąpić zablokowanie dostępu do konsoli zarządzającej z zewnątrz.

Uwaga!

W przypadku przywrócenia do ustawień fabrycznych urządzenia z NS-BSD 9 domyślne hasło dla użytkownika admin to 'admin'. W wersji 8 firmware'u hasło określane podczas pierwszego podłączenia.

Konfiguracja reguł filtrowania i translacji NAT

Dostęp do konfiguracji FILTER oraz NAT jest możliwy z poziomu *Security policy* -> *Filtering and NAT*.

Wspólne reguły

Konfiguracja sekcji FILTER i NAT zapisywana jest w jednej operacji przez silnik przetwarzania pakietów. Oznacza to, że konfiguracja, nawet jeśli jest przedstawiona w dwóch zakładkach, będzie zapisana we wspólnym pliku konfiguracyjnym.

Zasady działania FILTERING i NAT

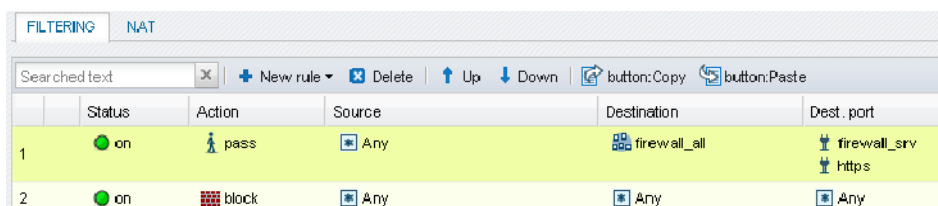
W firmwarze wersji 9, konfiguracja Filtering'u jest definiowana dla adresów IP (publiczne) przed ich modyfikacją przez moduł NAT. Zmiana kolejności działania modułów Filtering i NAT jest bardzo ważne dla budowania odpowiedniej polityki firewall. Na przykład (dla nowej wersji firmwaru 9) w celu umożliwienia dostępu do wewnętrznego serwera z sieci publicznej (np. Internetu) należy zdefiniować publiczny adres tego serwera w konfiguracji Filtering'u. To inne podejście od tego stosowanego w wypadku firmwaru w wersji 8, gdzie Filtering wymagał korzystania z serwera zdefiniowanego w oparciu o prywatny adres IP, a moduł filtrowania (firewall+IPS) działał po translacji NAT.

Harmonogram

Od firmwaru w wersji 9 harmonogram jest definiowany bezpośrednio w odniesieniu do konkretnej reguły, zdefiniowanej w sekcji Filtering, a nie jak dotychczas globalnie dla wszystkich reguł (slotu). W danej chwili aktywna jest jedna polityka, w ramach której reguły działają w oparciu o przypisany harmonogram. Ten z kolei jest reprezentowany przez nowy typ obiektów tzw. *Time object*.

Aktywna polityka po aktualizacji

W chwili aktualizacji urządzenia do firmwaru w wersji 9 ustawienia FILTERING i NAT zostaną przywrócone do ustawień fabrycznych. Na urządzeniu aktywna będzie tylko jedna polityka zezwalająca na administracyjne połączenie do urządzenia:



	Status	Action	Source	Destination	Dest. port
1	on	pass	Any	firewall_all	firewall_srv https
2	on	block	Any	Any	Any

IPSec VPN

Moduł IPSec został całkowicie zmieniony w wersji 9 celem uproszczenia konfiguracji tuneli VPN. Dotychczas tunele IPSec VPN należy zatem skonfigurować ponownie.

Konfiguracja bazy użytkowników

Od wersji 9 firmware'u dodatkowe atrybuty potrzebne do konfiguracji użytkowników są przechowywane lokalnie na urządzeniu. Co za tym idzie nie jest konieczna zmiana schematu zewnętrznej bazy danych Active Directory lub LDAP.

Obiekty

Migracja systemu zapewnia przeniesienie bazy obiektów z NS-BSD w wersji 8 do 9.

Status poszczególnych konfiguracji po wykonaniu aktualizacji

Konfiguracja	Firmware 9
Obiekty	Konfiguracja zachowana
Konfiguracja interfejsów	Konfiguracja zachowana
Routing	Konfiguracja zachowana
Dynamiczny DNS	Konfiguracja zachowana
Serwer DHCP	Ustawienia fabryczne
Klient NTP	Ustawienia fabryczne
DNS	Konfiguracja zachowana
SNMP	Częściowo zachowana
PPTP VPN	Konfiguracja zachowana
Powiadomienia e-mail	Ustawienia fabryczne
Klasyfikacja URL użytkownika	Konfiguracja zachowana
Filtering (Firewall i IPS)	Ustawienia fabryczne
Translacja NAT	Ustawienia fabryczne
IPSec VPN	Ustawienia fabryczne
Log configuration	Ustawienia fabryczne
Syslog/SMTP (alarms)	Ustawienia fabryczne
SSL VPN (servers)	Ustawienia fabryczne
SSL VPN (profiles)	Ustawienia fabryczne
QoS	Konfiguracja zachowana
Zdarzenia	Konfiguracja zachowana
Strefa czasowa	Konfiguracja zachowana
Uwierzytelnianie (Captive)	Ustawienia fabryczne
Antispam	Ustawienia fabryczne
Antivirus	Ustawienia fabryczne
Ruting dynamiczny	Konfiguracja zachowana
Active update	Konfiguracja zachowana
Secure configuration (Token)	Ustawienia fabryczne
Zdarzenia systemowe	Konfiguracja zachowana
System	Ustawienia fabryczne
LDAP (internal)	Ustawienia fabryczne
LDAP (external)	Konfiguracja zachowana
keytab (SPNEGO)	Konfiguracja zachowana
Uprawnienia administracyjne	Ustawienia fabryczne