Wykaz zmian w programie SysLoger

Pierwsza wersja programu 1.0.0.1 powstała we wrześniu 2011.

Funkcjonalność pierwszej wersji programu:

1. Zapis logów do pliku tekstowego,
2. Powiadamianie e-mail tylko dla wskazanych typów informacji/kategorii (alert, critical, error, warning, notice, info, debug).

– kod źródłowy programu zawiera ponad 1 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.2 (styczeń 2012):

1. Dodano definicje urządzeń, raportowanie według webfilteringu oraz logowań użytkowników,
2. Dodano powiadamianie według definicji fraz (pułapki w tekście logu),
3. Dodano wysyłanie powiadomień:
   - dla wskazanych kategorii webfilteringu,
   - dla wskazanych adresów IP sieci własnej,
   - z logowań użytkowników,
4. Dodano wykluczenia dla powiadomień,
5. Dodano możliwość definiowania webfilteringu z zaznaczeniem kategorii, która podlega powiadamianiu,
6. Dodano możliwość generowania raportów według:
   - webfilteringu,
   - własnych klas sieci,
   - zewnętrznych klas sieci,
   - typów wpisów (alert, critcal, error, warning, notice, info, debug),
   - aktualizacji czasu NTP na urządzeniach (informacja wykrywana na podstawie wpisu w logu),
   - zestawiania kanałów szyfrowanych (IKE),
   - logowań użytkowników (możliwość definiowania listy użytkowników),
7. Dodano możliwość definiowania własnych klas sieci,
8. Dodano możliwość definiowania zewnętrznych klas sieci,
9. Dodano możliwość definiowania adresów IP dla IKE,
10. Dodano dodatkowe parametry dla monitoringu adresów IP sieci własnej w zakresie usuwania fraz z tekstu oraz ignorowania fraz w tekście logu,
11. W zakresie adresów IP sieci własnej umożliwiono dopisanie adresu e-mail użytkownika do adresu IP, wskazanie adresu IP do ciągłego monitorowania oraz raportowania.

– kod źródłowy programu zawiera ponad 4 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.3 (marzec 2012):

1. Dodano obsługę bazy MySQL w tym tworzenie bazy, tabel, importowania z plików tekstowych, usuwania tabel, czyszczenia tabel, usuwania bazy,
2. Dodano warunkowe wykluczenia powiadomień dla adresów IP – wykluczenie działa na zasadzie wskazania ilości wystąpień w czasie (w sekundach),

3. Dodano możliwość tworzenia raportów na żądanie z pliku tekstowego oraz z bazy MySQL, raport z bazy MySQL zawiera wykresy dla typów (ogólny), typów według urządzeń, webfilteringu według urządzeń.

– kod źródłowy programu zawiera ponad 6 500 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.4 (marzec 2012):

1. Wersja zawiera poprawki funkcjonalne do wersji poprzedniej.

– kod źródłowy programu zawiera ponad 6 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.5 (sierpień 2013):

1. Dodano serwis PING, którego zadaniem jest sprawdzanie dostępności adresów IP w sieci wraz z powiadamianiem e-mail o braku odpowiedzi urządzenia,
2. Dodano serwis Nasłuch odpowiedzialny za możliwość definiowania uprawnionych adresów e-mail w celu dokonania kontroli dostępności adresu IP w sieci na podstawie odpowiednio przygotowanej i odebranej wiadomości e-mail z uprawnionego adresu e-mail, serwis zwrotnie wysyła wynik kontroli dostępności (15 prób).

– kod źródłowy programu zawiera ponad 7 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.6 (listopad 2013):

1. Rozbudowano opcje raportu z tekstowego pliku logu o możliwość raportowania z definiowanego zakresu dat,
2. Przebudowano opcje raportu z bazy MySQL dodając opcje raportowania według wcześniej zdefiniowanych parametrów:
   - kategorii,
   - webfilteringu,
   - klas własnych,
   - zewnętrznych klas,
   - IKE,
   - aktualizacji czasu NTP,
   - logowań użytkowników,
   - wskazanych adresów IP sieci własnej,
3. Dodano kontrolę dla możliwych ataków DDOS poprzez:
   - definiowanie granicznej wielkości pliku logu tekstowego (jedna wartość dla całego cyklu dziennego),
   - kontrolę ilości wpisów w czasie,
4. Rozbudowano opcje definicji urządzeń o możliwość dodania typu raportowania dla danego urządzenia (opcje wykorzystywane w raportowaniu z bazy MySQL).

– kod źródłowy programu zawiera ponad 10 400 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.7 (listopad 2013):

1. Dodano opcje filtrowania w oknie monitora według:
   - kategorii,

- urządzeń.

2. W oknie monitora dodano informację o zastosowanych filtrach,
3. Dodano opcje kontroli wolnego miejsca na dysku wraz z powiadamianiem e-mail w przypadku przekroczenia wartości krytycznej.

– kod źródłowy programu zawiera ponad 11 300 wierszy.

Modyfikacje/zmiany w wersji 1.0.1.0 (luty 2014):

1. Przebudowano program dodając obsługę działania syslog'a w serwisie systemu Windows. Funkcjonalność spowodowała uruchamianie serwisów i zapisywanie logów bezpośrednio po uruchomieniu systemu Windows bez konieczności logowania. Logowanie niezbędne w zakresie uruchomienia monitora oraz powiadomień e-mail,
2. Dodano opcje sterujące uruchomieniem serwisów:
   - syslog'a – odpowiedzialnego za odbiór logów z urządzeń, zapis w pliku tekstowym i/lub bazie MySQL, przesłanie logu do monitora,
   - raportowania –serwis odpowiedzialny za automatyczne wygenerowanie raportu o wskazanej godzinie na podstawie logu z pliku tekstowego z dnia poprzedniego według ustalonych parametrów i przesłanie na wskazany adres e-mail,
3. Przebudowano raporty według logów z plików tekstowych dodając możliwość przygotowania raportu według webfilteringu, ilości kategorii w czasie, dostępności urządzeń
4. Dodano wykresy graficzne dla raportu według logów w plikach tekstowych:
   - wykres/raport ilościowy braku dostępności,
   - wykres/raport procentowy dostępności,
   - wykres/raport kategorii,
   - wykres/raport kategorii w czasie,
   - wykres/raport webfilteringu.

– kod źródłowy programu zawiera ponad 18 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.1.1 (maj 2014):

1. Dodano możliwość definiowania numeru portu UDP nasłuchu monitora programu,
2. Przeniesiono opcje wykrywania ataków do odrębnej zakładki,
3. Dodano informacje o uruchomionych/zatrzymanych serwisach w zakładce „Serwisy",
4. Dodano serwis kopii konfiguracji wykorzystując działanie serwera TFTP oraz zewnętrznego programu plink w celu pobrania konfiguracji z urządzenia. Serwis umożliwia wykonanie kopii do dodatkowego repozytorium na innym serwerem.

– kod źródłowy programu zawiera ponad 20 600 wierszy.

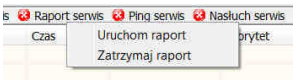
Modyfikacje/zmiany w wersji 1.0.1.2 (czerwiec 2014):

1. W głównym oknie monitora dodano:
   - prezentację uruchomienia poszczególnych serwisów,
   - informację o porcie nasłuchu monitora oraz uruchomienia serwisu Syslog'a,
   - możliwość uruchomienia i zatrzymania poszczególnych serwisów (rozbudowa przycisków Start i Stop)
2. Wprowadzono drobne zmiany graficzne.

– kod źródłowy programu zawiera ponad 21 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.2.0 (czerwiec 2014):

1. W głównym oknie monitora dodano opcje szybkiego uruchomienia i zatrzymania danego serwisu

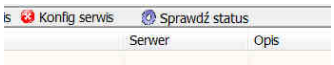


2. Dodano aplikację klienta monitora wraz z możliwością definiowania adresu IP i numeru portu nasłuchu. Klient monitora może być uruchomiony na innym zestawie komputerowym/laptopie/serwerze, jego zadaniem jest prezentowanie wpisów z logów syslog'a oraz informacji z usługi PING.

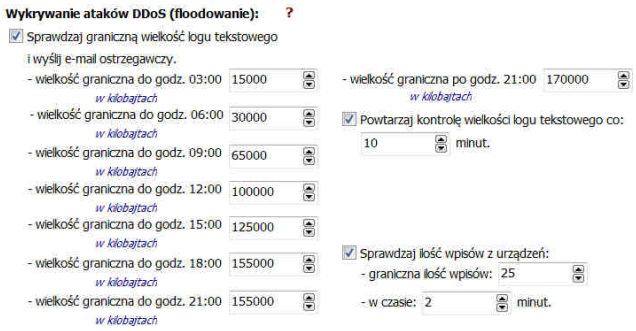
– kod źródłowy programu zawiera ponad 23 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.2.1 (listopad 2014):

1. W głównym oknie monitora dodano przycisk wymuszenia kontroli statusów poszczególnych serwisów



2. Rozbudowano opcje wykrywania ataków o dodatkowe kontrole wielkości logu pliku tekstowego



– kod źródłowy programu zawiera ponad 23 400 wierszy.

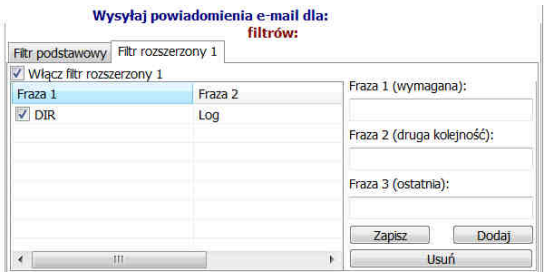
Modyfikacje/zmiany w wersji 1.0.3.0 (marzec 2015):

1. Poprawiono kontrolę działania bazy MySQL podczas uruchamiania okna monitora programu, skrócono czas uruchamiania okna monitora,
2. Dodano informację o logach działania programu: nazwa logu, wielkość logu,
3. Dodano opcje umożliwiające wyczyszczeni logów działania programu z pod samego programu.

– kod źródłowy programu zawiera ponad 24 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.3.1 (kwiecień 2015):

1. Przebudowano niektóre funkcje programu optymalizując kod źródłowy i działanie serwisu syslog, uzyskano poprawę wydajności podczas obsługi bazy MySQL,
2. Dodano filtr rozszerzony dla opcji powiadamiania umożliwiając wyszukiwanie dwóch lub trzech fraz w analizowanym logu z urządzenia

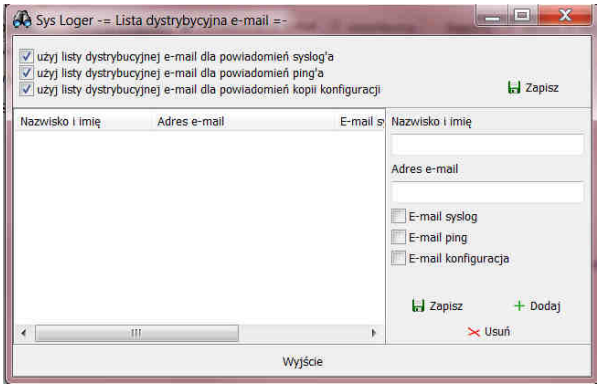


– kod źródłowy programu zawiera ponad 24 400 wierszy.

Modyfikacje/zmiany w wersji 1.0.4.0 (sierpień 2015):

1. Wprowadzono drobne zmiany graficzne,
2. Dodano dodatkową aplikację analizującą ruch w sieci na wskazanej karcie sieciowej (mini sniffer) – na ekranie prezentowane są informacje tylko adresie i porcie źródłowym i docelowym, wielkości pakietu, typie pakietu (TCP/UDP). Program nie zawiera pozostałych informacji w celu wyeliminowania możliwości sprawdzenia loginów czy haseł

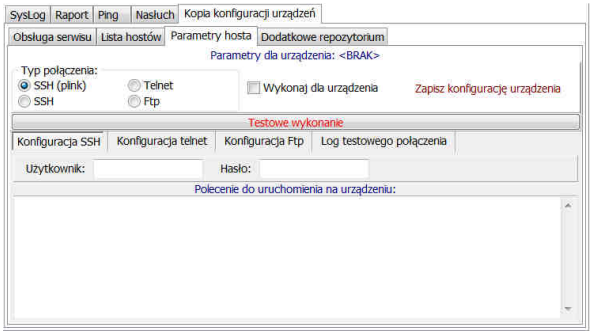
3. Dodano opcje definiowania listy dystrybucyjnej dla powiadomień e-mail w zakresie:
   - działania syslog'a,
   - dostępności urządzeń w sieci,
   - wykonania harmonogramu kopii konfiguracji



– kod źródłowy programu zawiera ponad 27 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.4.1 (wrzesień 2015):

1. W ramach serwisu kopii konfiguracji dokonano
   - przebudowy opcji sterujących w monitorze syslog'a



   - przebudowy serwisu kopii konfiguracji

- rozbudowy działania o wbudowane opcje SSH oraz FTP,
- zachowano możliwość wykorzystania zewnętrznego programu plink w celu łączenia protokołem SSH,
- zmieniono sposób łączenia w przypadku wykorzystania protokołu Telnet – zastosowano opcje wbudowane oraz szyfrowanie zawartości okna konfiguracji przy zapisie na dysku (ukryte zostały wszystkie polecenia w tym polecenia logowania, zmiany trybu na enabled).

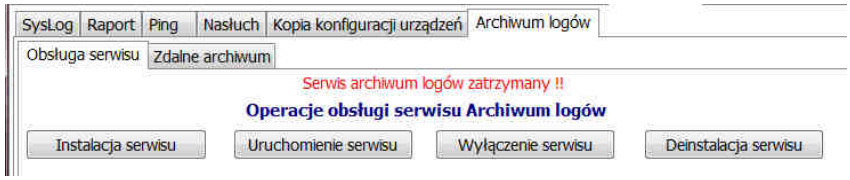
Uwaga !!! w przypadku korzystania z opcji Telnet dostępnej w poprzednich wersjach należy ponownie dokonać jej konfiguracji, zmianie uległ sposób jej obsługi – bez wprowadzenia zmian nie będzie możliwe wykonanie kopii konfiguracji z wykorzystaniem protokołu Telnet.

2. Dokonano optymalizacji w zakresie powiadamiania o wykonaniu konfiguracji, wprowadzono dodatkową kontrolę ilości wykonanych plików konfiguracji oraz wielkości plików konfiguracji. W przypadku niezgodności w temacie wiadomości e-mail dodano informację o błędzie oraz rodzaju błędu. Ograniczono ilość wiadomości e-mail do jednej podsumowującej.

– kod źródłowy programu zawiera ponad 28 100 wierszy.

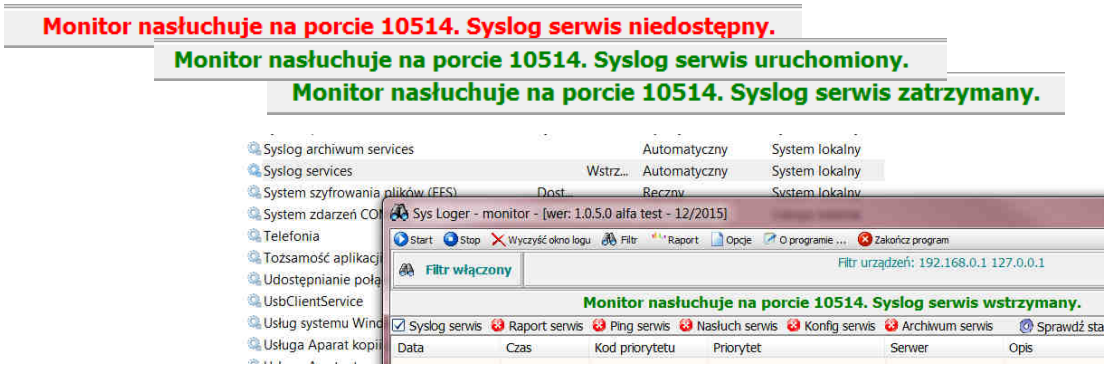
Modyfikacje/zmiany w wersji 1.0.5.0 (grudzień 2015):

1. Uruchomiono nową wersję klienta SSH – brak ograniczenia wielkości przesyłanego pliku,
2. Dokonano zmian graficznych oraz zmian w budowie raportów wysyłanych pocztą e-mail w zakresie powiadomień o dostępności urządzeń oraz raportów podsumowujących,
3. Uruchomiono archiwizację logów tekstowych z informacjami otrzymywanymi z urządzeń – konieczność wgrania i wskazania zewnętrznego programu do pakowania plików (na przykład 7za.exe w wersji ms-dos). Dodano możliwość zaszyfrowania/ukrycia wprowadzonych parametrów kompresji/dekompresji. Oryginalne logi tekstowe po spakowaniu są automatycznie usuwane – przed usunięciem następuje kontrola istnienia spakowanych plików oraz ich wielkości (usunięcie nastąpi jeżeli archiwum jest większe od zera),

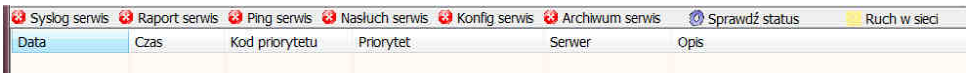


4. Dodano możliwość wykonania kopii spakowanych plików logów do zewnętrznego repozytorium. Zaimplementowano możliwość łączenia się protokołem FTP/SFTP/SMB. Obsługa repozytorium zewnętrznego następuje w momencie wykonania pakowania logów tekstowych,
5. Dodano obsługę spakowanych plików logów podczas wykonywania raportów. System dokonuje kontroli istnienia spakowanego archiwum, jego wypakowania – po czym wykonuje procesy raportowe i na końcu kasuje tekstowy plik logu wypakowany z archiwum. Do wypakowania archiwum uruchomiono dodatkowe pole w celu wprowadzenia parametrów de-kompresji (pole dostępne w obsłudze archiwum logów w zakładce serwisy). Wypakowanie następuje tym samym programem zewnętrznym, który dokonuje pakowania oryginalnych plików logów tekstowych,

6. W opcjach „Serwisy” dodano kontrolę instalacji (dostępności), zatrzymania oraz wstrzymania danej usługi/serwisu. Informacja jest prezentowana dla każdej usługi osobno w poszczególnych zakładkach: syslog, raport, ping, nasłuch, kopia konfiguracji urządzeń, archiwum logów. W głównym oknie monitora dodano również informację o statusie usługi syslog z podziałem na: niedostępny, uruchomiony, zatrzymany i wstrzymany. Status niedostępny zawsze oznacza brak zainstalowania danej usługi w systemie. W poprzedniej wersji była tylko informacja o uruchomieniu lub zatrzymaniu usług,



7. Dodano obsługę uruchomienia/zatrzymania usługi archiwum logów w głównym oknie monitora. W oknie głównym prezentowany jest też status uruchomienia usługi.



Uwaga. Procesy archiwizacyjne logów, w tym procesy obsługi zewnętrznego archiwum następują o godzinie 12:00 (obecnie godzina nadpisywana jest w pliku sysloger.ini przy każdym zapisie zmian, nie ma możliwości edycji godziny z pozycji programu). Archiwizacja i wysłanie do zewnętrznego archiwum obejmuje wszystkie tekstowe pliki logów za wyjątkiem pliku, do którego dokonywane są bieżące wpisy. Zaleca się aby godzina przygotowania codziennego raportu wykonywała się przed obsługą archiwum logów, tak aby dostępny był oryginalny plik logu. Kasowanie pliku logów po ich spakowaniu następuje z pominięciem systemowego „kosza”. Przed pierwszym uruchomieniem zaleca się dokonanie kopii wszystkich plików logów oraz zweryfikowanie prawidłowości wykonania pakowania i odzyskania plików.

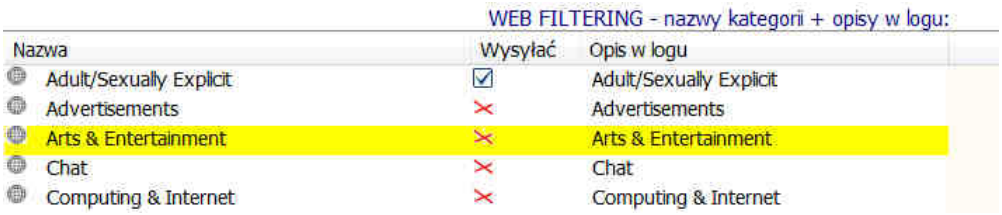
– kod źródłowy programu zawiera ponad 31 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.1 (luty 2016):

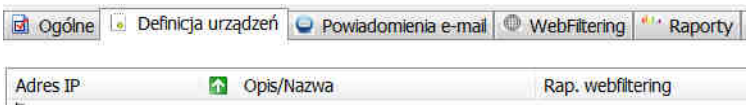
1. Poprawa wizualna zaznaczonych opcji poprzez zmiany w prezentacji danych pokazujących zestawienia na przykład: urządzeń, adresów IP, webfilteringu,

Rap. webfiltering	Rap. logowania / wystąpienia	Rap. własnych klas IP	Rap. zewnętrznych klas IP	Rap. IKE
☒	☒	☒	☒	☒
☑	☒	☒	☒	☒
☒	☒	☑	☒	☑
☑	☒	☑	☑	☑

gdzie: ikona ☒ oznacza brak wykonania, ikona ☑ oznacza wykonanie danego zadania.



2. Poprawiono odczyt listy adresów IP dla klienta monitora,
3. Zwiększono kolumny dla adresu IP oraz kolumnę nazwy dla definicji webfilteringu,
4. Dodano możliwość sortowania danych w prezentowanych listach – sortowanie odbywa się po kliknięciu w daną kolumnę (rodzaj sortowania pokazuje ikona w pasku danej kolumny):



5. Poprawa wizualna opcji wyboru dni w zakładce Serwisy -> Ping -> Lista hostów

– kod źródłowy programu zawiera ponad 32 300 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.2 (luty 2016):

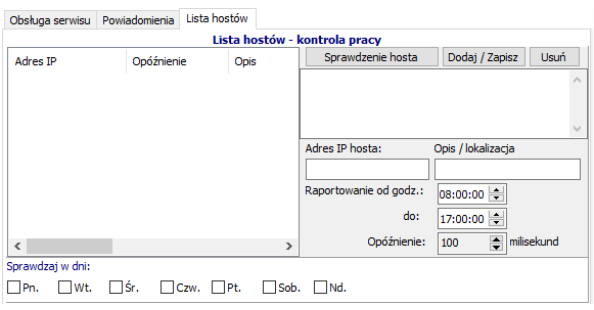
1. Poprawiono wysyłkę wiadomości e-mail w ramach list dystrybucyjnych,
2. Wprowadzono dodatkowy czas zwłoki 1 sekundy dla powtórzeń wykonania pakietu ICMP w procesie kontroli dostępności urządzeń w sieci eliminują przypadkowy błąd braku odpowiedzi,
3. Dodano obsługę testowania wiadomości e-mail dla włączonej opcji wysyłki za pomocą listy dystrybucyjnej

4. Poprawiono proces pobierania konfiguracji ustawień urządzeń za pomocą protokołu FTP.

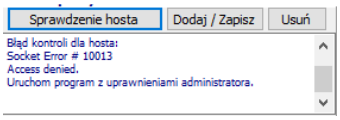
– kod źródłowy programu zawiera ponad 32 500 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.3 (kwiecień 2016):

1. Zmodyfikowano okno konfiguracji kontroli dostępności listy hostów (ping),
2. Zmodyfikowano procedurę kontroli dostępności hosta podczas wykonania testu uruchomianego przyciskiem „Sprawdzenie hosta”,

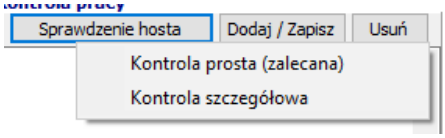


3. W przypadku wykrycia błędu z opisem „Access denied” podczas wykonania testu kontroli dostępności hosta dodano informację o konieczności uruchomienia programu z uprawnieniami administratora

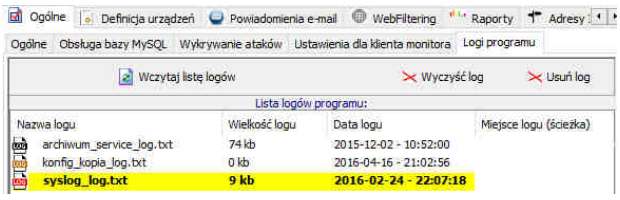


4. Zmodyfikowano format wiadomości e-mail generowanej podczas testu kontroli dostępności hosta,

5. Dodano możliwość edycji parametrów hosta w oknie konfiguracji kontroli dostępności (ping) – edycja możliwa jest po dwukrotnym kliknięciu lewym przyciskiem myszy na wybranym wierszu na liście hostów,
6. Dodano drugą (prostą) metodę wykonania testu dostępności hosta – metoda prosta korzysta z innych komponentów nie powodujących pojawianie się komunikatu błędu podczas zamknięcia programu (okna monitora). W przypadku wykonania kontroli metodą szczegółową należy koniecznie zamknąć i ponownie uruchomić program w celu wyeliminowania możliwego błędu podczas zaplanowanego automatycznego restartu programu i usług,



7. Uruchomiono obsługę roku i miesiąca w nazwach logów działania programu i poszczególnych usług dodając:
   - w nazwach plików logu działania programu elementów roku i miesiąca w formacie RRRR-MM,
   - kontrolę istnienia pliku logu działania i jego tworzenia w sposób ciągły
   - obsługę błędu podczas zapisów do plików logu działania programu.
8. Dodano log działania programu dla usługi ping_services, syslog_raport_services oraz zmieniono obsługę i nazwy pozostałych logów.
9. Zmodyfikowano okno przeglądania informacji o logach wprowadzając listę logów wraz z możliwością wyczyszczenia lub usunięcia wybranego logu. W oknie przeglądania dodano informację o ilości logów oraz łącznej wielkości w kilobajtach.



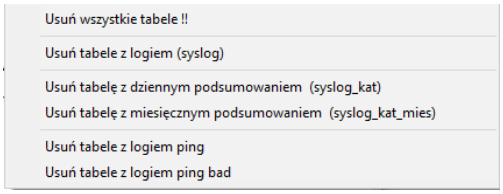
10. Dokonano aktualizacji wbudowanych komponentów SSH/SFTP zapewniając obsługę protokołu SSH2

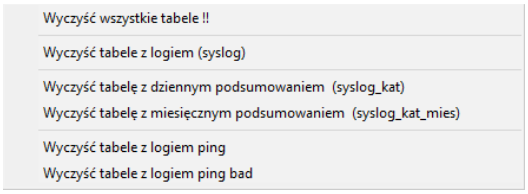
– kod źródłowy programu zawiera ponad 33 900 wierszy.

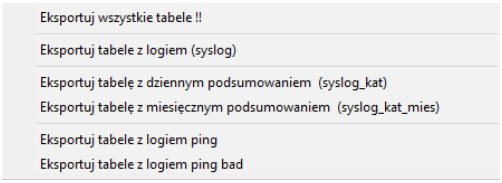
Modyfikacje/zmiany w wersji 1.0.5.4 (maj 2016):

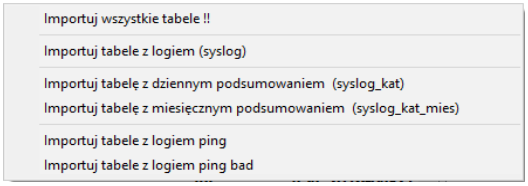
1. Dodano obsługę kolejnych tabel w bazie MySQL:
   - syslog_kat – tabela uzupełniania podczas wykonania codziennego raportu
   - syslog_kat_mies – tabela uzupełniania podczas wykonania codziennego raportu przy założeniu, że jest to ostatni dzień miesiąca,
   - syslog_ping – tabela uzupełniania wartościami minimalnymi, średnimi oraz maksymalnymi podczas wykonania kontroli dostępności urządzenia,
   - syslog_ping_bad – tabela uzupełniana informacją o braku dostępności urządzenia podczas wykonania kontroli,

   Rozszerzono obsługę w zakresie tworzenia, usuwania, czyszczenia, eksportowania oraz importowania tabel:





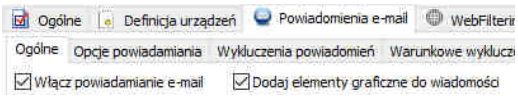




W przypadku uruchomienia obsługi bazy MySQL należy po wgraniu nowej wersji wykonać opcję „Utwórz tabele bazy danych" dostępną w zakładce Ogólne -> Obsługa bazy MySQL -> Parametry ogólne:

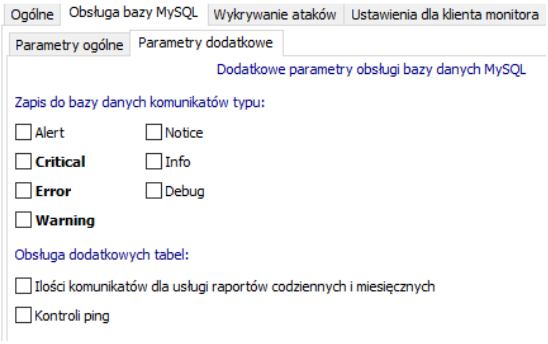
Podczas tworzenia tabel pominięte zostaną tabele już utworzone – dla takich tabel pojawi się komunikat o treści: Błąd tworzenia tabeli <nazwa tabeli>.

2. Zmodyfikowano usługę ping_services.exe dodając obsługę bazy MySQL w zakresie tabel: syslog_ping oraz syslog_ping_bad,
3. Dodano obsługę elementów graficznych w wiadomościach e-mail (ikony)



4. Obsługa bazy MySQL - dodano obsługę elementów graficznych w wiadomościach e-mail (ikony),

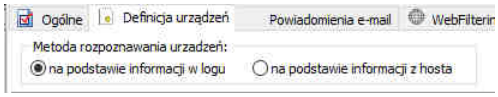
5. Rozszerzono zakładkę „Obsługa bazy MySQL” dodając dodatkowe zakładki „Parametry ogólne” oraz „Parametry dodatkowe”. W zakładce „Parametry ogólne” przeniesiono dotychczasowe opcje, w zakładce „Parametry dodatkowe” dodano elementy sterujące:
   - zapisem informacji do bazy MySQL w zakresie typów komunikatów: alert, critical, error, warning, notice, info, debug,
   - zapisem informacji dla dodatkowych tabel:
     - ilość komunikatów dla usługi raportów codziennych i miesięcznych – automatyczne podsumowania,
     - kontroli ping – zapis o poprawnym teście dostępu oraz o występujących błędach,



Dokonano implementacji obsługi nowych parametrów w poszczególnych usługach programu.

Uwaga. Po zainstalowaniu nowej wersji należy ponownie dokonać konfiguracji wszystkich parametrów obsługi bazy MySQL (domyślnie zapis do bazy uruchomiony jest tylko komunikatów typu alert, critical, error i warning).

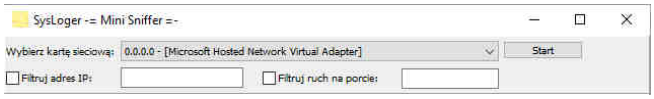
6. Podczas uruchomienia usługi syslog_services dodano kontrolę istnienia katalogu zapisu logów tekstowych. W przypadku braku istnienia wskazanego katalogu zapis logów następować będzie do podkatalogu „logi” znajdującego się w katalogu z programem,
7. Dodano możliwość ustawienia metody rozpoznawania urządzeń, do tej pory urządzenia rozpoznawane były na podstawie informacji uzyskiwanej w logu oraz wprowadzonej listy urządzeń (○ na podstawie informacji w logu). Wprowadzona druga metoda pozwala na uzyskiwanie informacji o urządzeniu na podstawie zestawionego połączenia – powiązania (○ na podstawie informacji z hosta)



Uwaga. Po instalacji nowej wersji należy zweryfikować prawidłowość definicji urządzeń, ich rozpoznawania w monitorze syslog’a oraz w tworzonych raportach dziennych.

8. Dodano obsługę znaku końca wiersza w treści message otrzymywanej z urządzeń. Znak końca wiersza jest automatycznie usuwany, znak końca wiersza może być dodawany przez niektóre systemy (na przykład systemy Linux/Unix),
9. SysLoger -=Mini sniffer=- rozbudowano funkcje kontrolujące ruch w sieci na danej karcie o możliwość filtrowania ruchu dla wskazanego adresu IP oraz numeru portu (funkcja filtruje

ruch dla adresu źródłowego oraz docelowego oraz dla numeru portu źródłowego i docelowego)



/program: syslog_mini_sniffer.exe/

10. Uruchomiono obsługę dodatkowego pliku INI: ping_hosts_status.ini, w którym zapisywane są informacje o statusie i dacie dostępności (obsługa uruchomiona w usłudze ping_services),
11. Dodano zapis informacji do dwóch dodatkowych logów tekstowych:
    - ping_bad_[yyyy-mm-dd].txt – zapis informacji o braku dostępu w formacie data i adres IP hosta,
    - ping_sred_[yyyy-mm-dd].txt – zapis informacji o poprawnym połączeniu w formacie data, adres IP hosta, wartość minimalna czasu odpowiedzi, średnia wartość czasu odpowiedzi, maksymalna wartość czasu odpowiedzi,
12. Kopia konfiguracji urządzeń – poprawiono proces weryfikacji poprawności wykonania poprzez uwzględnienie parametru wykonania dla danego urządzenia.

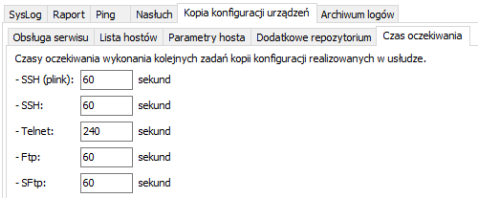
– kod źródłowy programu zawiera ponad 37 500 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.0 (październik 2016):

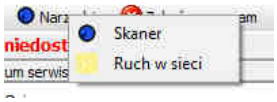
UWAGA !! Po instalacji nowej wersji konieczne jest ponowne wprowadzenie nazw użytkowników oraz haseł, parametrów kopii konfiguracji. Konieczność podyktowana przez nową wersją komponentów cipher oraz hashes, która zawiera obsługę Unicode.

1. Zmiana platformy – narzędzia developerskiego na DXe7 – analiza, dopasowanie w tym uruchomienie funkcji i procedur w nowej wersji oraz współpracy z nową wersją komponentów (między innymi: Indy 10.6.0.5169, Overbyte ICS v816, komponentów cipher i hashes v2.0.2010, Jedi 349, IP Works),
2. Obsługa bibliotek Open SSL dla połączeń SMTPS w wersji 1.0.2-i (openssl-1.0.2-i386-win32) z dnia 2015-01-24 (http://indy.fulgan.com),
3. Obsługa nowej biblioteki libmySQL oraz dbxmys.
4. Zapewnienie obsługi protokołu SMB (cifs) w zakresie braku interakcji z użytkownikiem dla systemu MS Windows 10 po jego aktualizacji w miesiącu lipiec 2016,
5. Dodano odświeżanie stanu serwisu: syslog, raport, ping, nasłuch, kopia konfiguracji, archiwum logów podczas wyświetlania poszczególnych zakładek,
6. Poprawiono działanie procedury sprawdzającej ping dla krótkich czasów powtórzeń, wykluczono możliwość ponownego uruchomienia procedury przed jej zakończeniem,
7. Poprawiono działanie procedur importu danych z plików tekstowych do tabel – dodano obsługę wskazanego w polu „Host bazy danych” serwera bazy MySQL (przed zmianą była obsługa tylko dla localhost),
8. Mini Sniffer – przygotowano osobną bibliotekę generującą listę interfejsów LAN,
9. Kopia konfiguracji – dodano obsługę wykonania kopii za pośrednictwem protokołu SFTP, poprawiono działanie w zakresie wykorzystania usługi telnet, dodano dodatkowy opis w logu

w przypadku błędu połączenia, dodano obsługę czasu oczekiwania na wykonanie kolejnego zadania kopii konfiguracji (czas podawany w sekundach).



10. Uruchomiono nowy moduł skanujący zasoby sieci – syslog skaner. W ramach wersji Demo możliwe jest wykonanie skanowania ręcznego dla maksymalnie 25 pierwszych adresów IP oraz skanowania automatycznego realizowanego wyłącznie w poniedziałek i/lub wtorek.

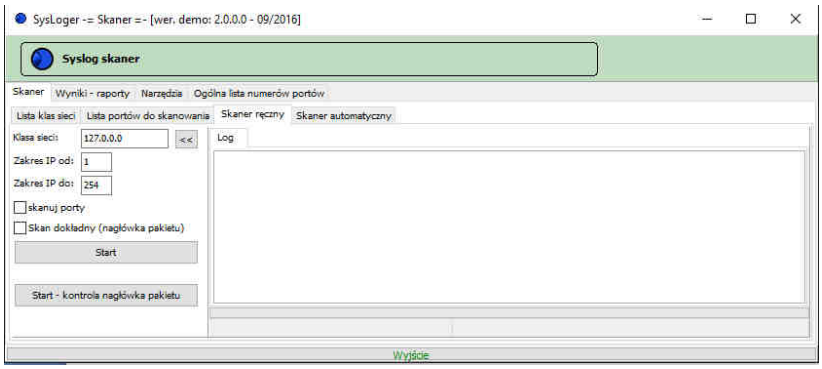


W głównym oknie dodano przycisk Narzędzia pozwalający uruchomić Skaner.

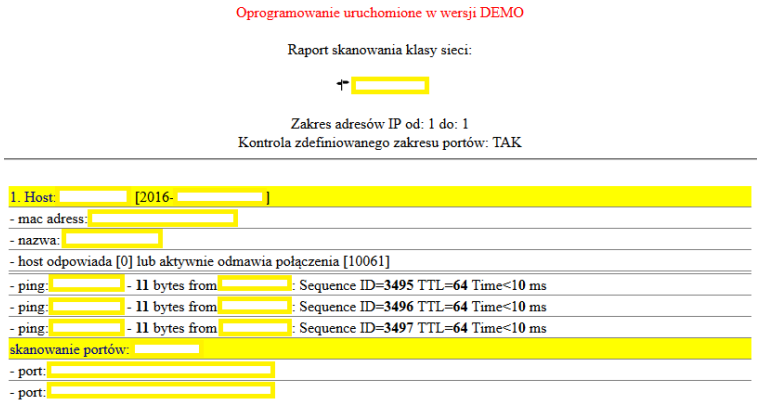
W ramach programu możliwe jest definiowanie:

- list klas sieci,
- listy portów objętych skanowaniem,
- parametrów skanowania automatycznego.

Program umożliwia przeprowadzenie skanowania ręcznego danej klasy sieci.



W trakcie skanowania [ręcznego/automatycznego] generowane są raporty w formacie HTML jak i tekstowym. Program generuje również raport nowych adresów IP z danej klasy sieci oraz prowadzi bazę zeskanowanych adresów oraz ich parametrów.


Oprogramowanie uruchomione w wersji DEMO

Raport skanowania klasy sieci:

Zakres adresów IP od: 1 do: 1
Kontrola zdefiniowanego zakresu portów: TAK

1. Host: [2016-]
- mac adress:
- nazwa:
- host odpowiada [0] lub aktywnie odmawia połączenia [10061]
- ping: - **11** bytes from : Sequence ID=**3495** TTL=**64** Time<**10** ms
- ping: - **11** bytes from : Sequence ID=**3496** TTL=**64** Time<**10** ms
- ping: - **11** bytes from : Sequence ID=**3497** TTL=**64** Time<**10** ms

skanowanie portów:
- port:
- port:

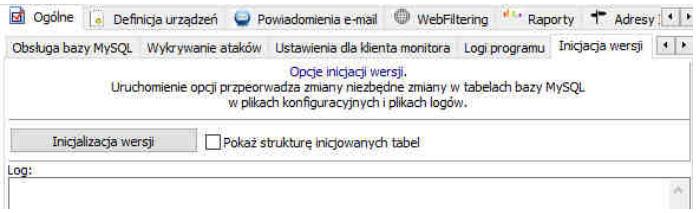
```
[          ]
data_dodania=2016
godzina_dodania=22:53:07
data_skanowania=2016
godzina_skanowania=13:07:49
ping_time=<10 ms
ping_bytes=11 bytes
ping_sequence_id=3497
ping_ttl=64
winsock_msg=host odpowiada [0] lub aktywnie odmawia połączenia [10061]
mac_adress=
nazwa=
```

– kod źródłowy programu zawiera ponad 42 800 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.1 (styczeń 2017):

Od wersji 2.0.0.1 po każdym wgraniu poprawek, nowej wersji należy wykonać inicjację wersji w celu wprowadzenia ewentualnych zmian w tabelach bazy MySQL, pozostałych plikach konfiguracyjnych lub raportach.

1. Uruchomienie opcji w nowej wersji komponentów Overbyte ICS v834,
2. Dodano opcje inicjacji wersji (Opcje -> zakładka: Ogólne -> Inicjacja wersji). Opcja inicjacji między innymi weryfikuje i dodaje obsługę dodatkowych kolumn w tabelach.



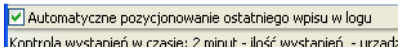
   Od wersji 2.0.0.1 konieczne jest uruchomienie opcji w celu uzupełnienia tabel bazy MySQL w zakresie wprowadzonych zmian.
3. Rozszerzono obsługę programu w zakresie komunikatów emergency,
4. Zmodyfikowano sposób obsługi bazy danych MySQL wprowadzając dodatkową kontrolę podczas pobierania danych,

– kod źródłowy programu zawiera ponad 43 700 wierszy.

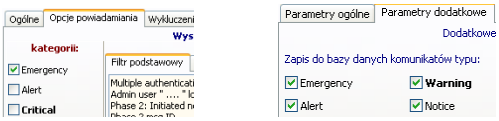
Modyfikacje/zmiany w wersji 2.0.0.2 (luty 2017):

1. Poprawa prezentacji działania usługi syslog serwis w oknie monitora,

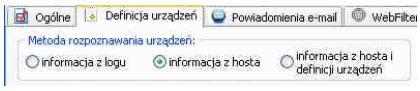
2. Dodano opcję automatycznego pozycjonowania ostatniego wpisu logu w oknie monitora,



3. Rozszerzono filtr okna logu, filtr powiadomień oraz filtr zapisu do bazy o opcje emergency,



4. Definicja urządzeń – dodano trzecią opcję rozpoznawania urządzeń: „informacja z hosta i definicji urządzeń” pozwalająca na dopisanie zdefiniowanej nazwy urządzenia do otrzymanego adresu IP,



5. Poprawiono metodę wyliczania i prezentacji informacji ilościowych dla urządzeń (zarejestrowanych i niezarejestrowanych).

– kod źródłowy programu zawiera ponad 43 800 wierszy.

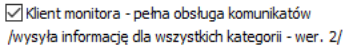
Modyfikacje/zmiany w wersji 2.0.0.3 (marzec 2017):

1. Dodano obsługę tworzenia kolejnych plików logów tekstowych w przypadku osiągnięcia wartości maksymalnej (wartość maksymalna tekstowego pliku logu to 2GB, w programie zaimplementowano możliwość ustawienia tej wartości na 1,5GB maks.), ustawiono maksymalną ilość plików logów dla danego dnia na 999,
2. Dodano obsługę raportów w zakresie kolejnych plików logów tekstowych
3. Zwiększono liczniki przetrzymujące ilościowe wystąpienia dla poszczególnych kategorii – maksymalna wartość licznika dla każdej z kategorii ustawiono na 500 mln wpisów,
4. Rozszerzono e-mail ostrzegający o osiągnięciu granicznej ilości wpisów w czasie o wpisy z logów z początkowego cyklu pomiarowego (warunkiem jest ustawienie kontrolnej wartości ilościowej pomiaru na minimum 20),

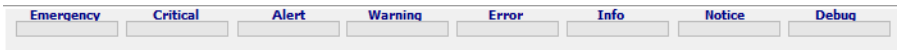
– kod źródłowy programu zawiera ponad 45 100 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.4 (lipiec 2017):

1. Dodano obsługę przekazywania informacji do programu winadmin_monitor (monitora przez WWW) w zakresie komunikatów z urządzeń oraz kontroli dostępności urządzeń,
2. Poprawiono obsługę pliku ini w zakresie działania programu do skanowania zasobów sieci,
3. Dodano raporty ze skanowania zasobów sieci (portów) dla pojedynczych adresów IP – raporty wykorzystywane w programie winadmin_monitor w celu prezentowania informacji dla danego adresu IP,
4. Dodano opcję pełną obsługę komunikatów przekazywanych do klienta monitora (wer. 2)



5. Rozbudowano opcje klienta monitora o prezentacje informacji ilościowej z każdej kategorii zdarzeń osobno (bez agregacji).



– kod źródłowy programu zawiera ponad 45 500 wierszy.