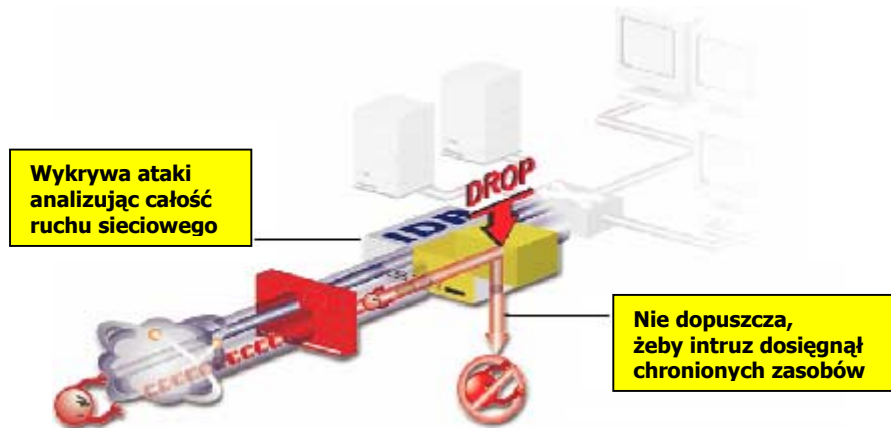


NetScreen-IDP™

System wykrywania intruzów i aktywnej ochrony



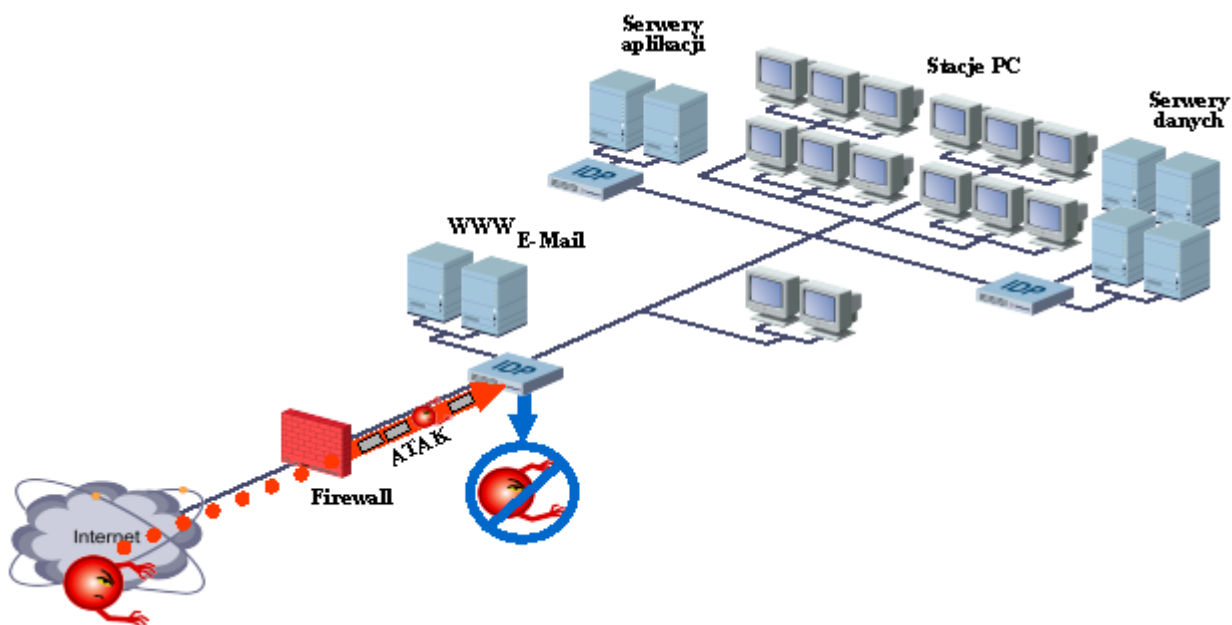
NetScreen-IDP to system zabezpieczeń sieciowych realizujący zadania wykrywania intruzów oraz w czasie rzeczywistym blokujący ataki. Należy do nowej klasy zabezpieczeń - *Intrusion Detection and Prevention (IDP)*. IDP potrafi skutecznie blokować ataki w odróżnieniu do zwykłych systemów IDS, które nasłuchując sieć identyfikują zdarzenia w czasie gdy intruzi wykonali już ataki na chronione zasoby i w praktyce nie są w stanie ich zablokować. Jest pierwszym na rynku systemem wykorzystującym osiem różnych metod detekcji ataków (m.in. *Stateful Signatures, Anomaly Detection, Network Honeypot, Spoofing Detection, Backdoor Detection*).

Własności:

- Umożliwia wykrywanie prób skanowania, penetracji i włamań, ataków typu Exploit (poziomu sieci i aplikacji), ataków destrukcyjnych typu (D)DoS oraz innych technik stosowanych przez hakerów.
- Posiada w pełni trójwarstwową architekturę - sensory, serwer zarządzania i interfejs GUI, umożliwiającą sprawne wdrożenie zabezpieczeń i zarządzanie bezpieczeństwem sieci.
- Może zostać wdrożony jako klasyczny IDS nasłuchujący sieć, bądź in-line IDS (bridge, router). Tryb in-line zapewnia, że analizowana jest całość ruchu i nie ma zagrożenia „zgubienia” pakietów przy większym obciążeniu sieci.
- Sensory IDP są dostarczane jako dedykowane, gotowe do wdrożenia urządzenia Appliance. Przepływność urządzeń wynosi ponad 500 Mb/s. Wydajność zabezpieczeń może zostać podwyższona do 2 Gb/s poprzez tworzenie klastrów, w których urządzenia współdzielą pomiędzy siebie ruch sieciowy.
- IDP wykrywa i blokuje intruzów przed osiągnięciem przez nich atakowanych systemów. Zwykły IDS nawet, jeżeli przekaże informacje o wykryciu ataku do systemu zaporowego Firewall to jest to już po fakcie.
- Baza IDP zawiera ponad 1500 sygnatur. Baza ta jest często aktualizowana przez producenta (min. raz w tygodniu). Nowe sygnatury ataków są centralnie instalowane na sensory w sieci z serwera zarządzania.
- Szeroki zakres reakcji IDS na zdarzenia (m.in. zablokowanie połączenia, reset sesji TCP, zarejestrowanie zdarzenia w logu, alarm, powiadomienie E-Mail i SNMP). Administratorzy mają możliwość definiowania własnych reakcji.
- Urządzenia IDP są wyposażone w karty wieloportowe i mogą poddawać kontroli wiele segmentów sieci jednocześnie. Obsługa sieci wirtualnych VLAN (802.1Q Tagging) i wirtualnych ruterów (Virtual Router), dzięki czemu pojedyncze urządzenie IDP może monitorować wiele punktów sieci bez ponoszenia przez firmę kosztów na zakup dodatkowych urządzeń i rekonfigurację infrastruktury sieciowej.
- Polityka bezpieczeństwa IDP składa się z opartego na logice zbioru reguł w odróżnieniu od „starej generacji” systemów IDS, których konfiguracja polega jedynie na włączaniu/wyłączaniu sygnatur ataków. Definiowanie reguł odbywa się za pomocą graficznego edytora polityki bezpieczeństwa. Reguły automatycznie instalują odpowiednie sygnatury na sensorach IDP.
- IDP posiada otwarty format sygnatur. Administratorzy mogą definiować własne sygnatury ataków i innych zdarzeń.
- Konsola administratora IDP umożliwia tworzenie graficznych i tekstowych raportów.
- Pomoc techniczna oraz szkolenia z produktu są dostępne w Polsce.

Techniki detekcji ataków

System zabezpieczeń IDP wykorzystuje wiele metod identyfikacji i ochrony przed atakami. Metody detekcji ataków włączone są w zależności od kontrolowanego ruchu sieciowego. Analiza danych za pomocą poszczególnych metod detekcji odbywa się w tym samym czasie (przetwarzanie współbieżne). Zapewnia to wysoką wykrywalność ataków bez obniżania wydajności.



Zastosowany w IDP mechanizm **Multi-Method Detection™ (MMD)** zawiera następujące metody detekcji:

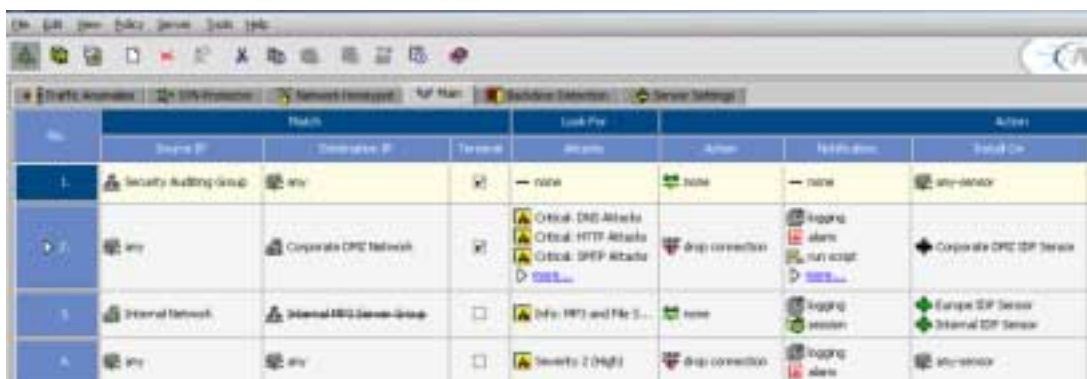
- *Stateful Signatures* - wykrywanie znanych ataków w oparciu o bazę sygnatur. Pełno-stanowe sygnatury zawierają dane na temat wzorca ataku oraz rodzaju komunikacji, gdzie takie zdarzenie może wystąpić. Ruch sieciowy poddawany jest analizie kontekstowej przez co w dużym zakresie eliminowane są fałszywe alarmy (tzw. false positives). Wzorce ataków wyszukiwane są tylko w wybranej komunikacji sieciowej, zapewniając w ten sposób dużą efektywność kontroli i wydajność zabezpieczeń.
- *Protocol Anomalies* - wykrywanie niezgodności ruchu sieciowego ze standardami określonych protokołów (m.in. RFC). W praktyce zdarza się, że intruzi w celu zmylenia zabezpieczeń, bądź ukrycia rzeczywistych ataków generują ruch sieciowy odbiegający od przyjętych norm i standardów.
- *Backdoor Detection* - wykrywanie aktywności "koni trojańskich" oraz prób nieupoważnionego dostępu do chronionych systemów poprzez tzw. "włazy" (backdoor). Detekcja odbywa się poprzez porównywanie ruchu sieciowego ze znanymi wzorcami działań intruzów oraz analizę heurystyczną transmitowanych pakietów.
- *Traffic Anomalies* - identyfikowanie działań w sieci, uznawanych za niedozwolone lub podejrzane, które są realizowane w formie wielu, różnych połączeń (np. skanowanie portów). Analizie poddawane są połączenia w określonych przedziale czasowym.
- *Spoofing Detection* - wykrywanie ruchu sieciowego ze sfałszowanymi adresami IP nadawcy pakietów (IP Spoofing). Intruzi często wykorzystują technikę IP Spoofing, żeby ukryć rzeczywiste źródło ataku. IDP wykrywa IP Spoofing porównując adresy IP w pakietach z adresami wykorzystywanymi w sieciach wewnętrznych.
- *Layer 2 Detection* - wykrywanie ataków i działań podejrzanych na poziomie warstwy 2 modelu OSI i adresacji MAC (np. ARP cache poisoning). Jest to szczególnie wartościowe w przypadku kontroli przez IDP sieci wewnętrznych.
- *Denial of Service Detection* - wykrywanie ataków destrukcyjnych i destabilizujących (Denial-of-Service, DoS). Ataki DoS realizowane są zwykle poprzez wysyłanie do serwera usługi dużej liczby odpowiednio spreparowanych zapytań, które wyczerpują jego zasoby (np. SYN-Flood).
- *Network Honeypot* - wczesne wykrywanie i rozpoznawanie działań intruzów poprzez stosowanie techniki "honeypot". IDP w trakcie skanowania, penetracji lub próby włamania do chronionego systemu przedstawia intruzom fikcyjne informacje nt. usług dostępnych na serwerach.

Zarządzanie i monitorowanie IDP

Serwer zarządzania IDP odpowiada za scentralizowane tworzenie i wdrażanie polityki bezpieczeństwa przedsiębiorstwa w zakresie wykrywania i blokowania ataków i innych działań niedozwolonych, a także konsolidowanie zdarzeń (logów, alarmów) rejestrowanych na wielu sensorach w sieci i składowanie ich w centralnej bazie danych. Administratorzy z dowolnego miejsca w sieci mogą zarządzać całym systemem IDP z użyciem dedykowanych, graficznych narzędzi.

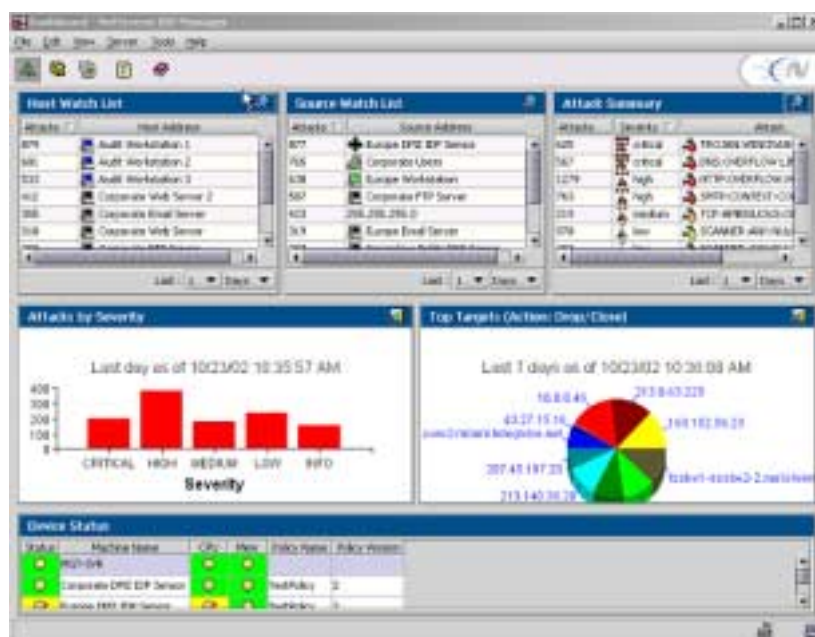
Konsola zarządzająca IDP składa się z sześciu podstawowych komponentów:

- *Security Policy Editor* - edytor polityki bezpieczeństwa umożliwiający tworzenie różnego rodzaju reguł (m.in. *Main*, *SYN-Protector*, *Network Honeypot*, *Backdoor Detection*, *Traffic Anomalies*, *Sensor Settings Rulebases*) i wdrażanie ich na wybrane sensory IDP w sieci.
- *Dashboard* - wyświetla w czasie rzeczywistym najbardziej istotne statystyki z funkcjonowania sieci i zabezpieczeń. Zawiera następujące sekcje: *Host Watch List*, *Source Watch List*, *Attack Summary*, *Reports* i *Device Status*.
- *Object Editor* - zarządzanie obiektów, na których operuje system zabezpieczeń IDP. Do podstawowych obiektów można zaliczyć *Network Object* (np. sieć, host, serwer, sensor), *Service Object* (np. FTP, HTTP, Telnet) oraz *Attack Object* (np. sygnatury ataków i anomalii protokołów).



Konsola zarządzania IDP umożliwia wdrożenie jednej, centralnej polityki bezpieczeństwa sieci przedsiębiorstwa w zakresie wykrywania intruzów i aktywnego blokowania ataków

- *Log Viewer* - przeglądanie i analizowanie zdarzeń rejestrowanych przez sensory IDP zgodnie z ustaloną polityką bezpieczeństwa. Wyświetla rekordy logów w formacie tabeli z możliwością definiowania specyficznych reguł filtracji i selekcji danych.
- *Device Monitor* - przedstawia aktualny stan sensorów IDP i serwera zarządzania (m.in. procesora, pamięci operacyjnej, procesów zabezpieczeń) oraz alarmuje administratora w razie wystąpienia sytuacji wyjątkowych.
- *Reports* - generuje różnego rodzaju raporty na podstawie zdarzeń zarejestrowanych przez sensory IDP.



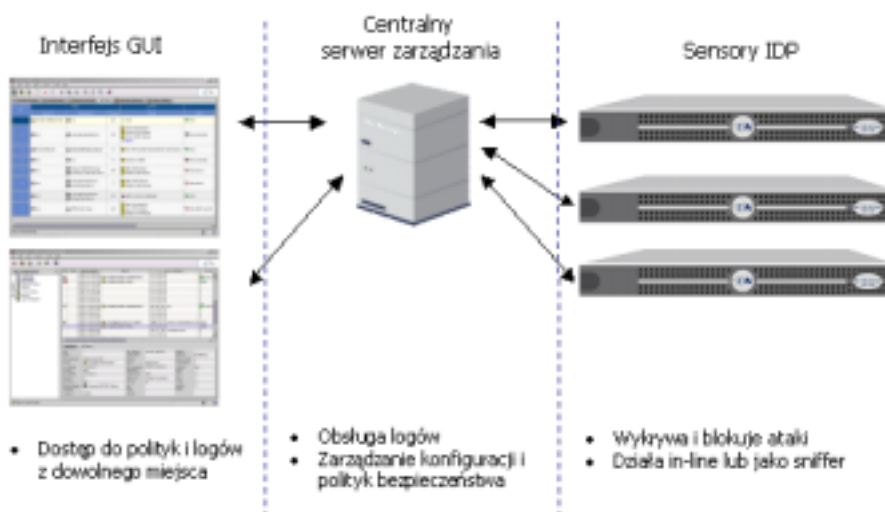
Graficzna konsola IDP na bieżąco przedstawia aktualny stan bezpieczeństwa sieci

Architektura IDP

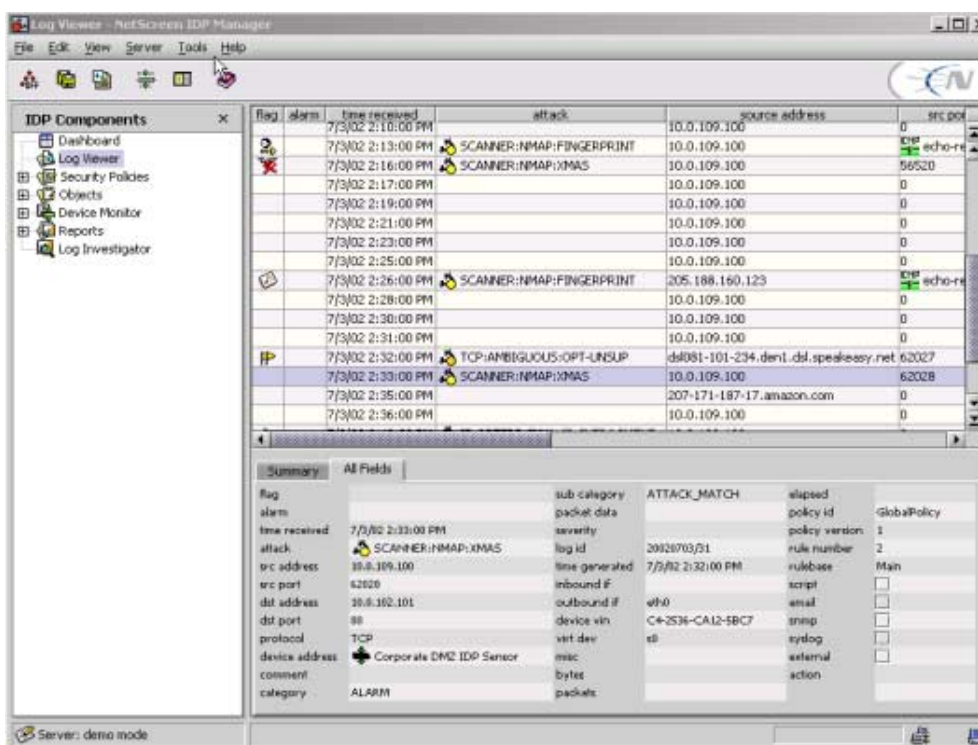
System zabezpieczeń IDP posiada w pełni trójwarstwową architekturę - sensory, serwer zarządzania i interfejs GUI. Umożliwia ona sprawne wdrożenie zabezpieczeń i zarządzanie bezpieczeństwem sieci.

IDP składa się z następujących komponentów:

- *Sensory IDP* - analizują całość ruchu sieciowego, wykrywają i blokują ataki oraz wymuszają ustaloną politykę bezpieczeństwa,
- *Serwer zarządzania (IDP Management Server)* - przechowuje i zarządza wszystkimi sygnaturami ataków, bazą logów oraz zbiorem polityk bezpieczeństwa.
- *Interfejs GUI* - graficzne narzędzia do zarządzania IDP, umożliwiające administratorowi wykonywania swoich zadań z dowolnego miejsca w sieci.



System IDP może zostać wdrożony w architekturze rozproszonej (tzn. wszystkie komponenty oddzielnie) lub scentralizowanej, gdzie serwer zarządzania i sensor IDP funkcjonują na jednym urządzeniu. Całość zarządzania IDP oraz obsługa logów odbywa się na centralnym serwerze zarządzania. Polityki bezpieczeństwa są tworzone na serwerze zarządzania i instalowane na sensory IDP w sieci. Komunikacja sieciowa pomiędzy wszystkimi komponentami IDP jest zabezpieczona kryptograficznie. Sensory IDP mogą funkcjonować w trybie in-line lub sniffer. Pracując w trybie in-line sensory IDP mogą zostać wdrożenie w architekturze odpornej na awarie (*High Availability, HA*).



Administrator IDP analizuje zdarzenia zarejestrowane w różnych miejscach sieci przez sensory

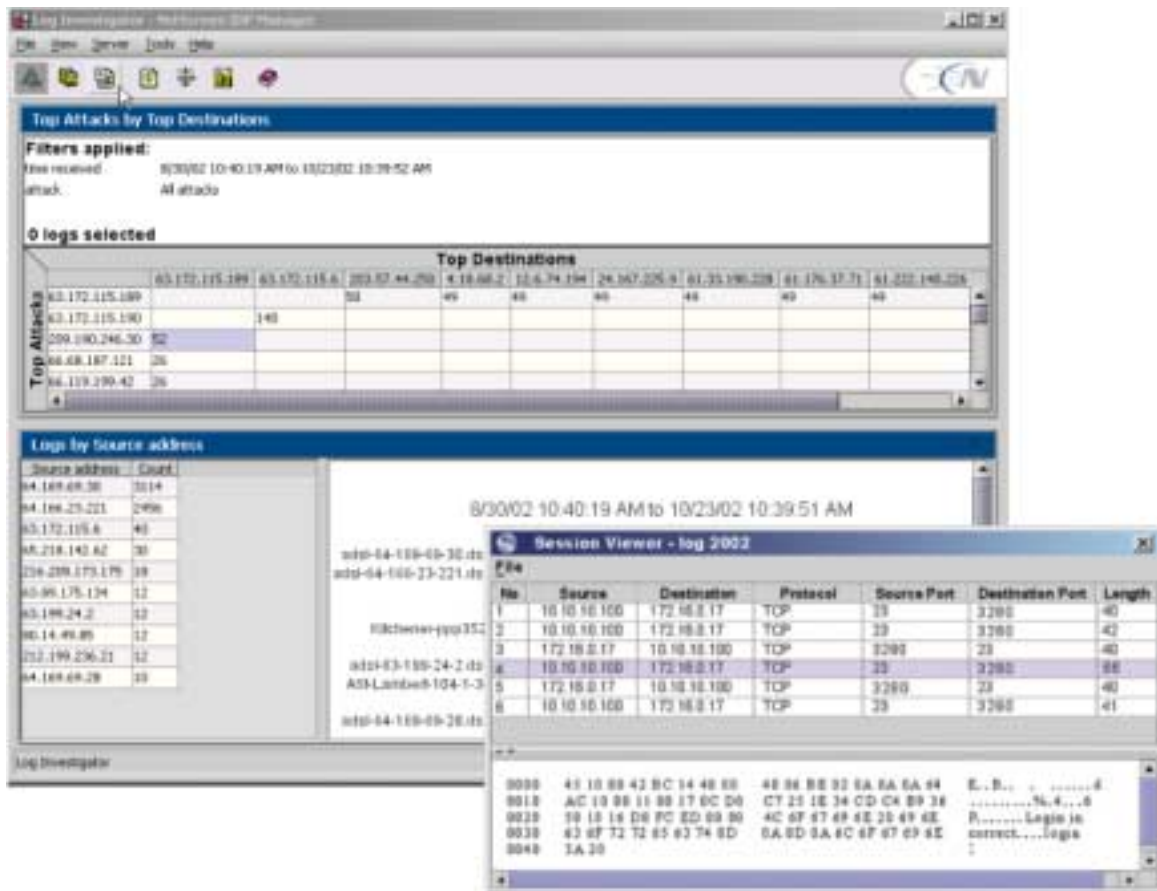
Analiza bezpieczeństwa sieci

System IDP w czasie rzeczywistym wykrywa niedozwolone i podejrzane działania jak skanowanie, próby penetracji i włamań, ataki typu *Exploit* (poziomą siecią i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz wiele innych technik stosowanych przez hakerów. Detekcja ataków odbywa się z użyciem różnych metod stosowanych w zależności od rodzaju analizowanego ruchu.

flag	alarm	time received	attack	source address	src p...
		7/3/02 5:08:00 AM		10.0.109.100	0
		7/3/02 6:13:00 AM		10.0.0.44	0
		7/3/02 6:25:00 AM		10.0.0.44	0
🚩		7/3/02 6:25:00 AM	SMTP:CONTEXT:CONFIDENTIAL	Europe Workstation	2046
🕒		7/3/02 6:32:00 AM		10.0.109.100	IDP echo-
🕒		7/3/02 7:04:00 AM	TROJAN:WINCRASH:SERVER-RES	Internal Workstation	35946
🕒		7/3/02 7:08:01 AM	HTTP:CGI:ORACLE-WEB-REMOTE-EXEC	dsl081-101-100.den1.dsl.sneakeasy.net	2047
🕒		7/3/02 7:11:00 AM	HTTP:ISS:OUTLOOK-WEB-DOS	dsl081-101-100.den1.dsl.sneakeasy.net	2051
		7/3/02 7:19:00 AM	HTTP CGI: Oracle Web Listener Batch Remote Exec	...eakeasy.net	2055
		7/3/02 8:02:00 AM	SMTP:...	...eakeasy.net	2055
		7/3/02 9:05:00 AM	HTTP:...	...eakeasy.net	2056
		7/3/02 11:21:00 AM			0
🚩		7/3/02 12:20:00 PM	MP3:N...		0
		7/3/02 2:10:00 PM			0
		7/3/02 2:10:00 PM		10.0.109.100	0

Narzędzia IDP umożliwiają wykonanie dokładnej analizy bezpieczeństwa sieci

Administrator dokonuje analizy bezpieczeństwa systemu informatycznego z użyciem dedykowanych narzędzi. Za pomocą *Log Viewer* przegląda i selekcjonuje zdarzenia zarejestrowane przez sensory IDP. Specjalne narzędzia *Log Investigator* umożliwiają dokładne rozpoznanie sposobu prowadzenia i zakresu ataków.



Administrator IDP wyjaśnia zaistniałe incydenty i podejrzane zdarzenia z użyciem Log Investigator

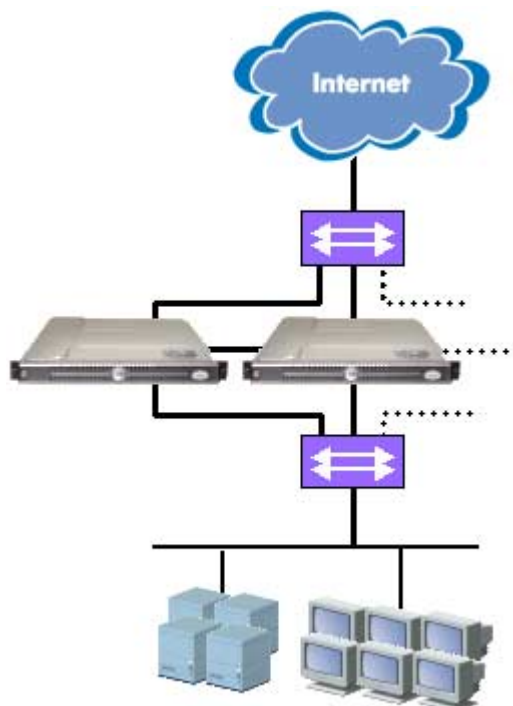
Ochrona przed awariami

System zabezpieczeń IDP może zostać wdrożony w konfiguracji odpornej na awarie - *High Availability (HA)*. Konfiguracji HA składa się z dwóch lub więcej urządzeń IDP tworzących klastery, które kontrolują się wzajemnie i w razie wystąpienia awarii przejmują zadania uszkodzonej maszyny. Kłaster HA złożony z wielu urządzeń IDP (od 2 do 16) zapewnia dostępność zabezpieczeń w razie awarii oraz zwiększa wydajność systemu poprzez równoważenie ruchu sieciowego (*load balancing*).

Wdrożenie konfiguracji HA może odbywać się z wykorzystaniem różnych metod, m.in.:

- *Stand-alone HA*,
- *Spanning Tree Protocol (STP)*,
- zewnętrzne urządzenie *Load Balancer*.

Kłaster HA może funkcjonować w trybie *Hot-Standby* (tzw. gorąca rezerwa), bądź też w trybie *Active-Active*, gdzie wszystkie urządzenia IDP są aktywne. Informacje o stanie kontroli ruchu sieciowego są w czasie rzeczywistym współdzielone pomiędzy urządzeniami IDP w klastrze HA za pomocą dedykowanego protokołu synchronizacji. Urządzenia posiadają także specjalnie do tego celu opracowane mechanizmy wykrywania awarii i automatycznego przejmowania zadań uszkodzonej maszyny.



Wymagania systemowe

System zabezpieczeń IDP składa się z trzech warstw ochrony – sensory IDP, centralny serwer zarządzania oraz interfejs GUI. Sensory IDP dostarczane są jako gotowe do użycia urządzenia Appliance. Wymagania systemowe do wdrożenia serwera zarządzania i konsoli GUI zostały przedstawione poniżej.

Sensory IDP:

Model	NetScreen-IDP 10	NetScreen-IDP 100	NetScreen-IDP 500
<i>Interfejsy inspekcyjne:</i>			
10/100 Fast Ethernet	2	2 (rozszerzalne do 8)	Brak (rozszerzalne do 8)
Gigabit Ethernet (F.O.)	Brak	Brak (rozszerzalne do 2)	2
Gigabit Ethernet (miedź)		Opcjonalnie	Opcjonalnie
<i>Interfejsy zarządzania:</i>			
10/100 Fast Ethernet	1	2	2
Pamięć (RAM)	512 MB	1 GB	4 GB
Maksymalna liczba sesji	10,000	70,000	220,000
Wydajność	20 Mb/s (do 100 Mb/s)	200 Mb/s	500 Mb/s
<i>Redundancja fizyczna:</i>			
Zasilacz zapasowy	Nie	Opcjonalnie	Tak
RAID	Nie	Opcjonalnie	Tak

Serwer zarządzania:

- System operacyjny: Solaris 7/8, RedHat Linux 7.2
- Procesor: 1GHz (Linux), 400 MHz (Solaris)
- Pamięć RAM: 512 MB

Interfejs GUI:

- System operacyjny: Windows 2000, RedHat Linux 7.2
- Pamięć operacyjna: 256 MB



Dystrybucja w Polsce:

CLICO Sp. z o.o., Al. 3-go Maja 7, 30-063 Kraków
 Tel: +12 6325166; +12 2927525; Fax: +12 6323698
 E-mail: support@Clico.PL, orders@Clico.PL.;
 Ftp.clico.pl.; http://www.clico.pl