



BEZPIECZEŃSTWO SIECI ZARZĄDZANIE

Zasady i dobre praktyki projektowania zabezpieczeń sieciowych Intrusion Prevention

Opracował: Mariusz Stawowski, CISSP

Email: mariusz.stawowski@clico.pl

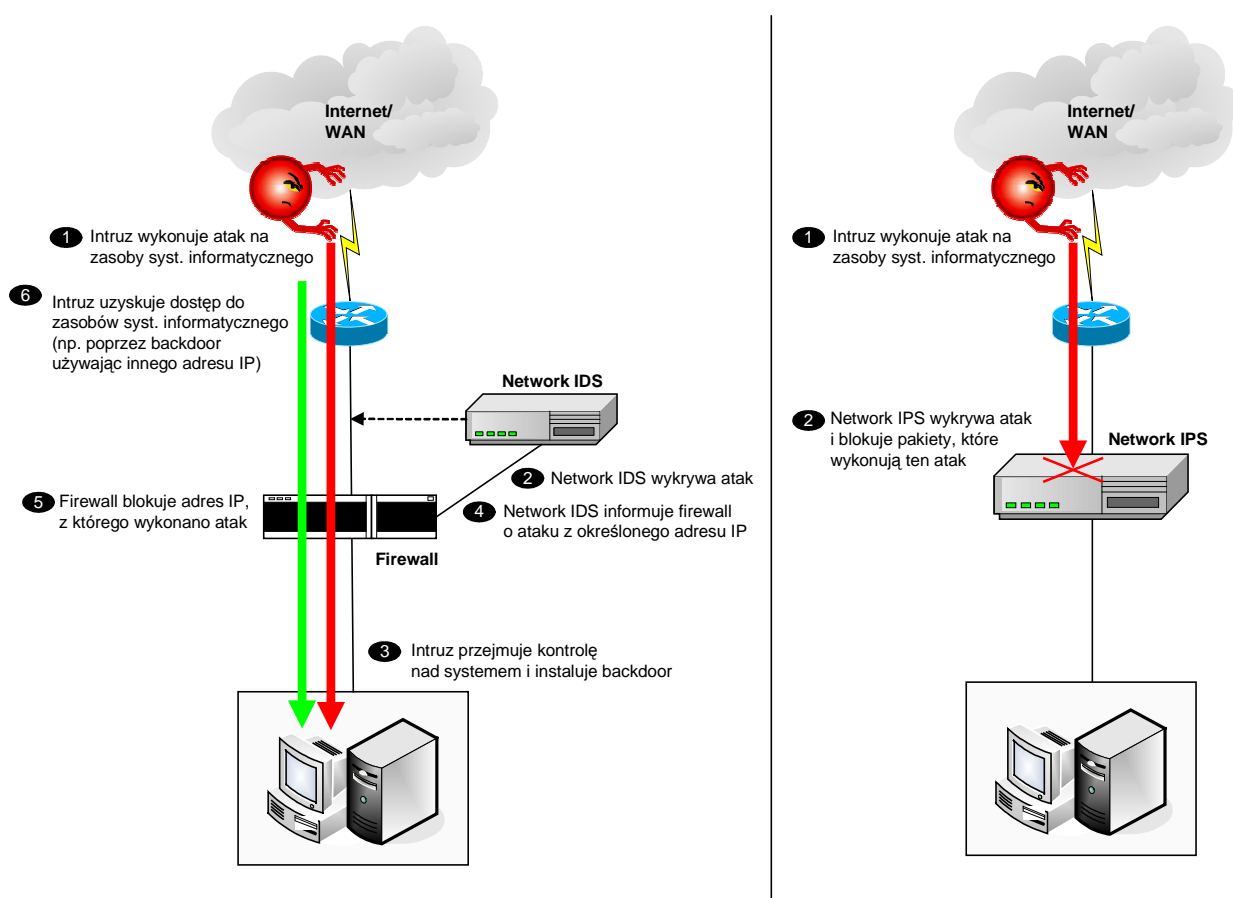
12.11.2006.

Spis treści

1. WPROWADZENIE	3
2. TYPOWE SCENARIUSZE WŁAMAŃ	5
3. ZASADY I ETAPY PROJEKTOWANIE ZABEZPIECZEŃ IPS	9
4. OPRACOWANIE INFRASTRUKTURY ZARZĄDZANIA ZABEZPIECZEŃ	15
5. USTALENIE POLITYKI ZABEZPIECZEŃ IPS	16
6. PROJEKTOWANIE SKALOWANYCH I NIEZAWODNYCH ZABEZPIECZEŃ IPS	19
7. OBSŁUGA INCYDENTÓW BEZPIECZEŃSTWA	23
8. OPRACOWANIE PLANU TESTÓW AKCEPTACYJNYCH	24
Literatura	25

1. Wprowadzenie

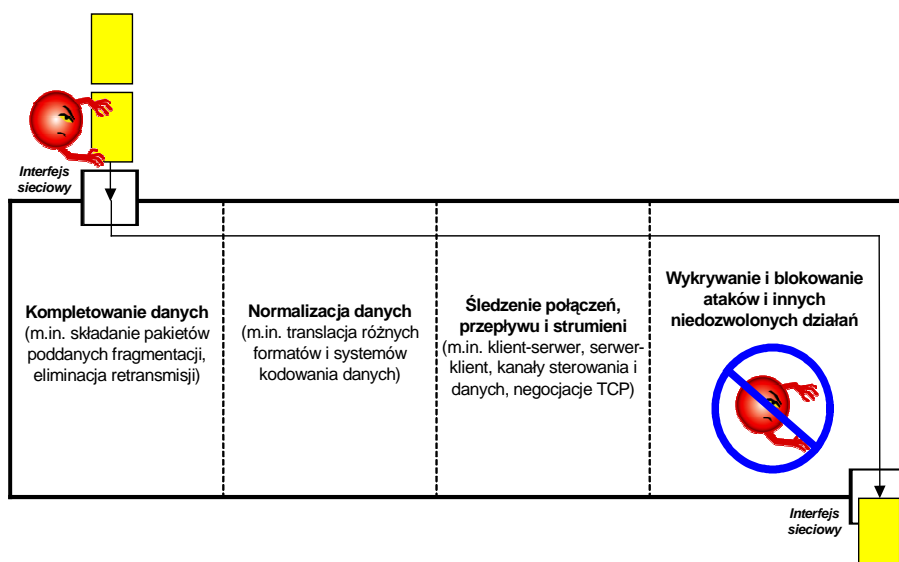
Zapewnienie właściwej ochrony przed zagrożeniami z sieci to obecnie podstawowe wymaganie bezpieczeństwa w systemach informatycznych. Pojawiają się coraz doskonalsze techniki penetracji i włamań, takie jak ataki hybrydowe oraz szybko rozprzestrzeniające się w sieci inteligentne robaki i Trojany. W sieci Internet dostępne są łatwe w obsłudze narzędzia do wykorzystywania podatności (np. Metasploit). Zabezpieczenia starej generacji jak Network IDS (*ang. intrusion detection system*) działające na zasadzie nasłuchu sieci, czy firewalle typu Stateful Inspection nie radzą sobie z tymi zagrożeniami.



Rysunek 1. Porównanie działania sieciowego IPS z IDS zintegrowanym z firewallem

Od systemów zabezpieczeń wymagane jest wykrywanie ataków i ich skuteczne blokowanie. Zabezpieczenia tej klasy określane są jako IPS (*ang. intrusion prevention system*). Pierwszą ich implementacją były systemy Host IPS. Nie przyjęły się one jednak w powszechnym zastosowaniu, ponieważ sprawiają problemy ze stabilnością i wydajnością pracy chronionych serwerów i w praktyce nie blokują wielu ataków. Oprogramowanie Host IPS jest bowiem instalowane bezpośrednio na serwerach i przez to stwarza ich dodatkowe obciążenie i może powodować zakłócenia pracy. Atak na system komputerowy (np. przez exploit) jest zwykle wykonywany w bardzo krótkim czasie. Jest to jednokrotne połączenie z serwerem i uruchomienie na nim złośliwego kodu. W praktyce za pomocą zabezpieczeń Network IDS nawet zintegrowanych z systemem firewall (*tzw. firewall signaling*) nie ma możliwości blokowania ataków. Jedyne skuteczne w tym zakresie środki ochrony to Network IPS. Mimo pozornego podobieństwa Network IDS zintegrowany z firewallem zachowuje się zupełnie inaczej niż Network IPS i w rzeczywistości stwarza większe zagrożenie niż korzyści. Różnicę tę najlepiej zrozumieć analizując popularne scenariusze włamań do systemów informatycznych. Zasady działania obu rozwiązań ochrony przedstawia rysunek 1. Porównanie skuteczności dedykowanego systemu Network IPS i IDS zintegrowanego z firewallem można łatwo przeprowadzić nawet z wykorzystaniem prostej sieci testowej.

Systemy IPS są w stanie skutecznie, w sposób aktywny przeciwstawiać się atakom intruzów funkcjonując w trybie in-line. Zasady działania Network IPS są podobne do systemów firewall. Ruch wchodzi do urządzenia IPS przez interfejs sieciowy i wewnątrz jest poddawany analizie, a następnie wychodzi z urządzenia innym interfejsem. Dzięki temu kontrola ruchu sieciowego jest łatwiejsza, pojawia się mniej niż w przypadku urządzeń IDS fałszywych alarmów i co najważniejsze całkowicie eliminowane jest zagrożenie, że IPS „zgubi pakiety”. Najistotniejsze jest jednak, że w trybie in-line ataki mogą być w czasie rzeczywistym blokowane przed ich dotarciem do chronionych zasobów systemu informatycznego. Rysunek 2 przedstawia zasady kontroli ruchu sieciowego w systemie zabezpieczeń IPS na przykładzie rozwiązania Juniper Networks Intrusion Detection and Prevention™ (IDP). Analiza ruchu sieciowego w IDP odbywa się w oparciu o stosowane w zależności od potrzeb i konfiguracji różne techniki detekcji m.in. *Stateful Signatures, Protocol Anomalies, Network Honeypot, Backdoor Detection, Traffic Anomalies, Spoofing Detection, Layer 2 Detection* i *Denial of Service Detection*.



Rysunek 2. Zasady kontroli ruchu sieciowego w systemie zabezpieczeń IDP

Do podstawowych funkcji bezpieczeństwa realizowanych przez systemy zabezpieczeń IPS można zaliczyć:

- wykrywanie i blokowanie penetracji i ataków wykonywanych przez intruzów i robaki internetowe (tzn. aplikacje samodzielnie włamujące się do systemów komputerowych),
- monitorowanie stanu bezpieczeństwa (m.in. wykrywanie niedozwolonych działań i powiadamianie administratorów),
- wspomaganie administratorów w zakresie wyjaśniania zaistniałych naruszeń bezpieczeństwa (m.in. korelacja zdarzeń i generowanie raportów).

Zaawansowane rozwiązania IPS umożliwią wdrożenie innych środków ochrony. Dla przykładu, system zabezpieczeń IDP posiada następujące funkcje bezpieczeństwa, m.in.:

- oszukiwanie intruzów poprzez techniki typu 'honeypot',
- blokowanie Spyware, Keylogger i innych złośliwych aplikacji (Malware),
- wykrywanie nieupoważnionych komputerów podłączonych do sieci wewnętrznej,
- nadzorowanie przestrzegania przez pracowników przyjętej polityki bezpieczeństwa (np. wykorzystywania niedozwolonych aplikacji),
- wspomaganie administratorów w zakresie wykrywania systemów i aplikacji podatnych na błędy bezpieczeństwa,
- wykrywanie sytuacji „przełamania zabezpieczeń” (m.in. identyfikowanie połączeń z Backdoor za pomocą technik analizy heurystycznej oraz nowo otwartych portów na serwerach specyficznych dla Trojanów i Backdoor).

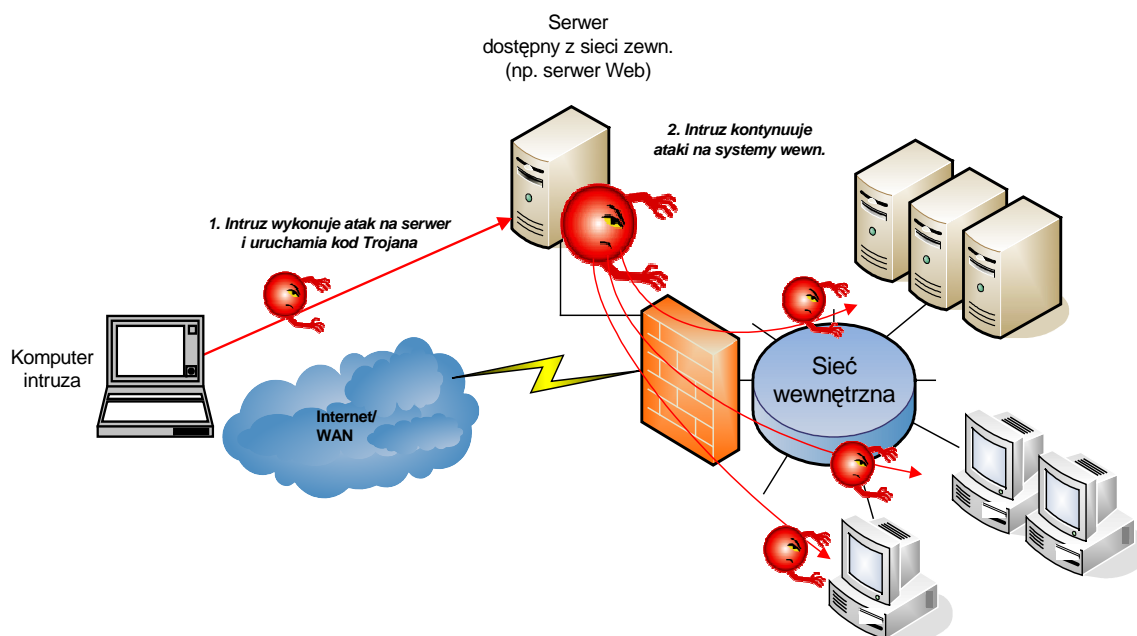
2. Typowe scenariusze włamań

Wdrożenie w systemie informatycznym skutecznych zabezpieczeń Intrusion Prevention wymaga znajomości możliwych scenariuszy włamań i uwzględnienia ich w projekcie zabezpieczeń. Zasoby systemu informatycznego narażone są na wiele, różnego rodzaju niebezpieczeństw, najczęściej wynikających z globalnego charakteru oraz dużego skomplikowania środowiska sieci komputerowych (np. Internet, intranet, ekstranet). Obserwowane w Internecie ataki intruzów zwykle rozpoczynają się od penetracji i przejęcia kontroli nad serwerem publicznym firmy (np. Web, SMTP, DNS). Serwery takie w większości firm znajdują się w wydzielonym segmencie sieci tzw. DMZ. Wykonanie włamania na serwer jest możliwe, gdy oprogramowanie tego serwera posiada błąd umożliwiający uruchamianie poleceń systemowych. Można w ten sposób skopiować na serwer aplikację typu Trojan (np. CAFEiNi, G@du-Ghost, Luzak, SKUN, Wspomagacz) i uruchomić ją w celu uzyskania zdalnego dostępu do systemu. Błąd oprogramowania serwera implementowany jest zwykle w specjalnej aplikacji, popularnie nazywanej exploit. Po przejęciu kontroli nad serwerem intruz może wykonywać na nim różnego rodzaju działania (np. Web graffiti) lub kontynuować atak na inne strefy bezpieczeństwa (np. sieć wewnętrzną). Taktyka przejmowania kontroli nad kolejnymi strefami bezpieczeństwa w sieci nosi nazwę *Island Hopping Attack*.

Można wyróżnić dwa typowe scenariusze włamań:

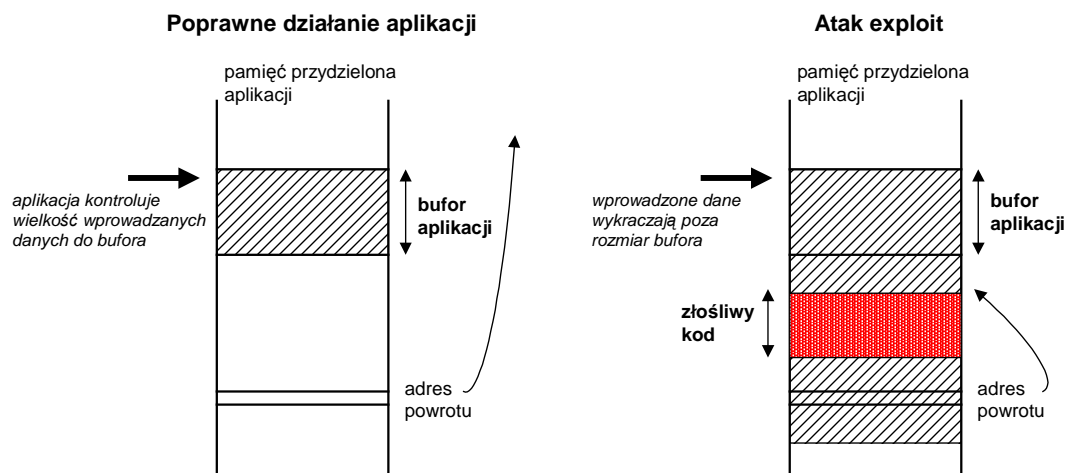
- włamanie bezpośrednie do systemu z wykorzystaniem błędu aplikacji sieciowej (tzw. włamanie przez exploit),
- włamanie za pomocą aplikacji przesłanej do sieci wewnętrznej (tzw. włamanie przez agenta).

W razie przejęcia kontroli nad systemem następuje zainstalowanie w systemie aplikacji intruza i kontynuowanie za jej pomocą penetracji sieci wewnętrznej. Do tego celu mogą zostać wykorzystane popularne aplikacje Trojan lub podmieniające pliki systemowe komputera, trudne do wykrycia aplikacje Rootkit.



Rysunek 3. Koncepcja włamania do systemu poprzez exploit

Najczęściej stosowaną metodą w atakach exploit jest przepełnienie bufora (*ang. buffer overflow*). Technika polega na zapisaniu do bufora aplikacji dużej wielkości danych tak, aby nastąpiło jego przepełnienie i nadpisanie obszaru pamięci za buforem. Zwykle aplikacja otrzymuje w ten sposób nowy kod do wykonania. Atak exploit polega na wprowadzeniu do pamięci i wykonaniu złośliwego kodu. Z uwagi na rodzaj buforów wykorzystywanych w atakach wyróżnia się dwie techniki ataku - rozbijanie stosu (*ang. stack smashing*) oraz rozbijanie sterty (*ang. heap smashing*).



Rysunek 4. Koncepcja ataku exploit poprzez przepełnienie bufora

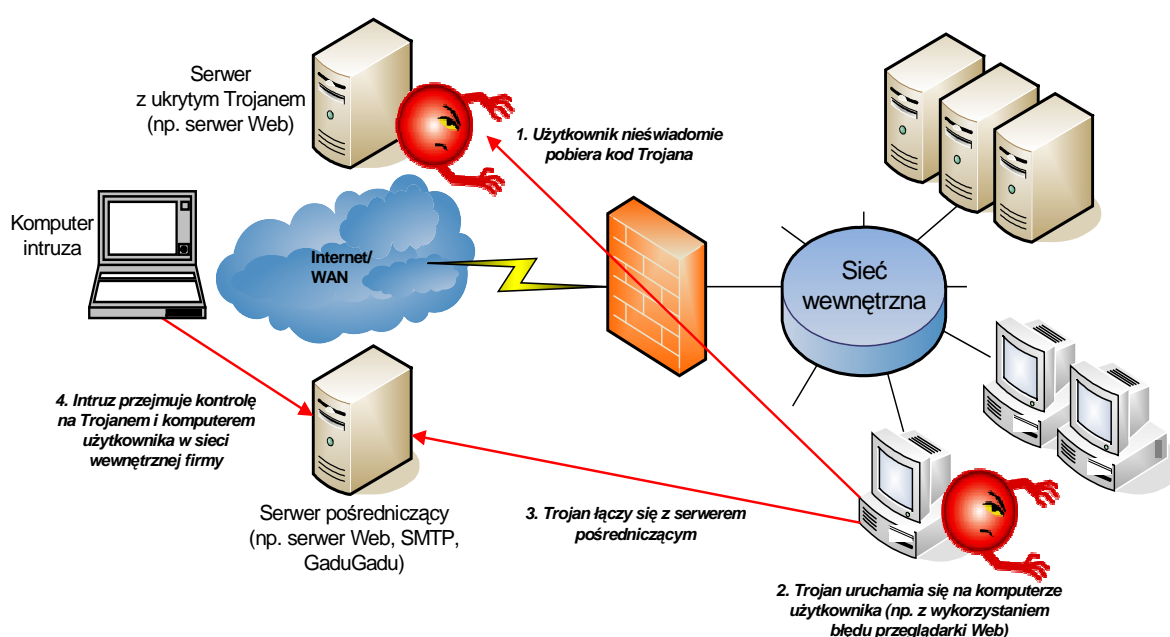
Aplikacja uruchomiona w komputerze ma do dyspozycji określony rozmiar pamięci, z której korzysta w trakcie wykonywania swoich funkcji (m.in. przetwarzania danych). Dane aplikacji są składowane w obszarach pamięci określanych jako bufor. W pamięci zapisany jest także adres, który określa gdzie aplikacja powinna przejść po zakończeniu bieżącej funkcji tzw. adres powrotu. Poprawnie napisana aplikacja kontroluje dane wprowadzane do bufora i nie pozwala na przekroczenie jego dopuszczalnego rozmiaru. Jeżeli jednak aplikacja nie jest właściwie napisana istnieje możliwość wprowadzenia danych przekraczających dopuszczalną wielkość bufora. Rysunek 4 przedstawia koncepcję ataku exploit poprzez przepełnienie bufora. Intruz wprowadza do pamięci kod do wykonania (np. uruchomienie Backdoor na określonym porcie TCP) i zmienia adres powrotu funkcji tak, aby kod został uruchomiony. W konsekwencji intruz przejmuje kontrolę nad systemem komputerowym.

Kompletny scenariusz typowego włamania do sieci wewnętrznej firmy poprzez exploit przebiega w następujący sposób:

- rozpoznanie celu ataku (m.in. skanowanie portów, TCP/IP fingerprint),
- przejęcie kontroli nad systemem (zwykle serwerem w strefie DMZ),
- instalacja aplikacji Trojan/Backdoor,
- penetracja systemu, kradzież i modyfikacja danych oraz kontynuowanie ataków na inne zasoby systemu informatycznego.

Wykonując projekt zabezpieczeń sieciowych IPS należy rozumieć w jaki sposób następuje przejęcie kontroli nad atakowanym systemem. Po wykonaniu ataku exploit, załadowaniu i uruchomieniu kodu (*shellcode*) nawiązywane jest połączenie z atakowanym systemem. Może się to odbywać poprzez połączenie z wskazanym portem TCP/UDP, na którym został uruchomiony kod lub poprzez połączenie zwrotne z komputerem intruza. Projektowane zabezpieczenia IPS powinny być przygotowane na takie sytuacje.

Włamanie przez agenta (nazywany także 'bot') polega na przesłaniu do sieci wewnętrznej firmy złośliwego kodu (*ang. malicious code*). Odbywa się to zwykle za pomocą ogólnie dostępnych usług sieciowych. Dla przykładu, pocztą elektroniczną można przesłać do określonego użytkownika kod JavaScript lub ActiveX jako zawartość wiadomości e-mail napisanej w języku HTML. W razie stosowania przez użytkownika nieaktualnej wersji klienta poczty lub przeglądarki Web, bądź też ich niewłaściwej konfiguracji (np. pozwalającej na wykonywanie bez ograniczeń aplikacji ActiveX) uruchomiony kod dokona skopiowania plików użytkownika, bądź innych niebezpiecznych działań. Kod uruchomiony przez klienta poczty na komputerze użytkownika może próbować wykonać niedozwolone operacje lub uruchomić przeglądarkę Web, która z komputera intruza załaduje i uruchomi inny złośliwy kod (np. Trojana).



Rysunek 5. Koncepcja włamania do systemu za pomocą agenta

Kod agenta może zostać także przesłany do sieci wewnętrznej za pomocą bardziej zaawansowanych technik jak np. Phishing lub Pharming. Użycie techniki Phishing w tym przypadku polega na wysłaniu do pracowników firmy wiadomości email w imieniu zaufanej im osoby (poprzez technikę *email spoofing* i inżynierię społeczną), zachęcającej do odwiedzenia określonej strony Web. Dla przykładu, email od administratora lub szefa informatyki może zachęcać pracowników do wejścia na stronę Web w celu przetestowania nowej aplikacji, gdzie w rzeczywistości intruz umieścił kod exploit na przeglądarkę Web wraz z Trojanem. Technika Pharming atakuje serwis DNS (serwery DNS lub lokalne ustawienia komputera w pliku 'hosts') w taki sposób, aby na zapytanie DNS o zaufany serwer Web otrzymany został adres IP serwera spreparowanego przez intruza, na którym umieszczony został kod exploit atakujący przeglądarkę Web wraz z agentem, który zainstaluje się na komputerze użytkownika w wyniku uruchomienia exploit.

3. Zasady i etapy projektowanie zabezpieczeń IPS

Wdrożenie skutecznych, skalowalnych i efektywnych kosztowo zabezpieczeń IPS dla średniej i dużej wielkości systemu informatycznego wymaga ich odpowiedniego zaprojektowania. Network IPS jest elementem systemu zabezpieczeń sieciowych, który stanowi wzmocnienie i uzupełnienie innych środków bezpieczeństwa istniejących w systemie informatycznym (m.in. zabezpieczeń firewall, mechanizmów ochrony w systemach operacyjnych, bazach danych i aplikacjach). Przed wdrożeniem zabezpieczeń należy przeprowadzić specyfikację wymagań bezpieczeństwa (m.in. analizę ryzyka) i ustalić, m.in.:

- które zasoby systemu informatycznego podlegają ochronie przed atakami (np. serwery w sieci wewnętrznej, serwery DMZ),
- jakie są istotne zagrożenia zasobów i gdzie znajdują się ich źródła (np. włamania i ataki DoS z Internetu, włamania z sieci oddziałowych przez VPN),
- jaka powinna być reakcja zabezpieczeń na ataki (np. alarmowanie, blokowanie ataków),
- gdzie powinny być zlokalizowane zabezpieczenia (np. w strefie DMZ, przed firewallem, w sieci wewnętrznej).

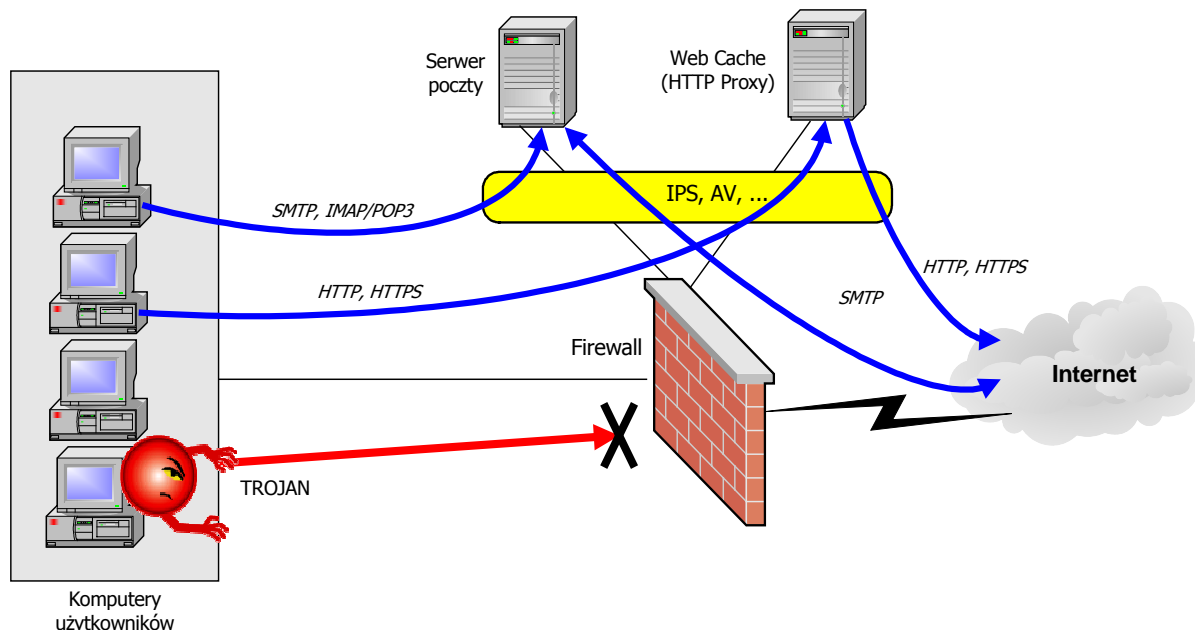
W trakcie projektowania zabezpieczeń sieciowych IPS należy uwzględnić następujące fundamentalne zasady bezpieczeństwa systemów informatycznych¹ [1-2, 4, 7, 9-11]:

- **"Compartmentalization of Information"** - zasoby systemu informatycznego o różnym poziomie wrażliwości (tzn. wartości i podatności na zagrożenia) powinny znajdować się w różnych strefach bezpieczeństwa. Rozszerzeniem tej zasady jest zasada "Information Hiding" mówiąca, że z systemu informatycznego udostępniane są dane tylko takie, które są konieczne do realizacji zadań systemu informatycznego.
- **"Defense-in-Depth"** – ochrona wrażliwych zasobów systemu informatycznego opiera się na wielu warstwach zabezpieczeń. Rozszerzeniem tej zasady są następujące zasady²: "Layered Protections" – warstwy zabezpieczeń uzupełniają i ubezpieczają się wzajemnie; "Defense in Multiple Places" – warstwy zabezpieczeń znajdują się w różnych miejscach systemu informatycznego.
- **"The Principle of Least Privilege"** – użytkownicy i administratorzy systemu informatycznego posiadają minimalne uprawnienia, które umożliwiają poprawne funkcjonowanie instytucji. Zasada odnosi się także do danych i usług udostępnianych użytkownikom zewnętrznym. Rozszerzeniem tej zasady jest zasada "Need-To-Know" mówiąca, że użytkownicy i administratorzy systemu inf. posiadają dostęp do informacji, wynikający z zajmowanego stanowiska i aktualnie realizowanych zadań służbowych.
- **"Weakest link in the chain"** – poziom bezpieczeństwa systemu informatycznego zależy od najsłabiej zabezpieczonego elementu tego systemu.

¹ Wykonując projekt zabezpieczeń sieciowych należy mieć na uwadze także zasady odnoszące się do organizacji bezpieczeństwa m.in. "Seperation of Duty" i "Job Rotation", które mają za zadanie ograniczyć pracownikom możliwości naruszeń bezpieczeństwa. Zasad "Seperation of Duty" mówi, iż ważne zadania/funkcje powinny być wykonywane przez dwóch lub więcej pracowników. Zasada "Job Rotation" mówi, że na ważnych stanowiskach powinna występować rotacja pracowników.

² Znana jest także zasada "Defense Through Diversification", rozszerzająca zasadę „Defense-in-Depth”, która mówi iż bezpieczeństwo zasobów systemu informatycznego powinno opierać się na warstwach ochrony złożonych z różnego rodzaju zabezpieczeń. Jeżeli występują dwie warstwy tego samego rodzaju zabezpieczeń to powinny pochodzić od różnych producentów. Zasada ta powinna być stosowana ostrożnie, ponieważ zwiększa skomplikowanie systemu zabezpieczeń, przez co utrudnia jego właściwe zarządzanie i utrzymanie.

Istotne dla ochrony przed intruzami są odpowiednio zaprojektowane strefy bezpieczeństwa oraz ustawienia kontroli dostępu. Komputery użytkowników w sieci wewnętrznej nie powinny mieć możliwości zawiązywania bezpośredniego połączenia z Internetem tak, aby w razie przesłania do użytkownika Trojana nie mógł on nawiązać połączenia z intruzem (patrz scenariusz włamania przez agenta).

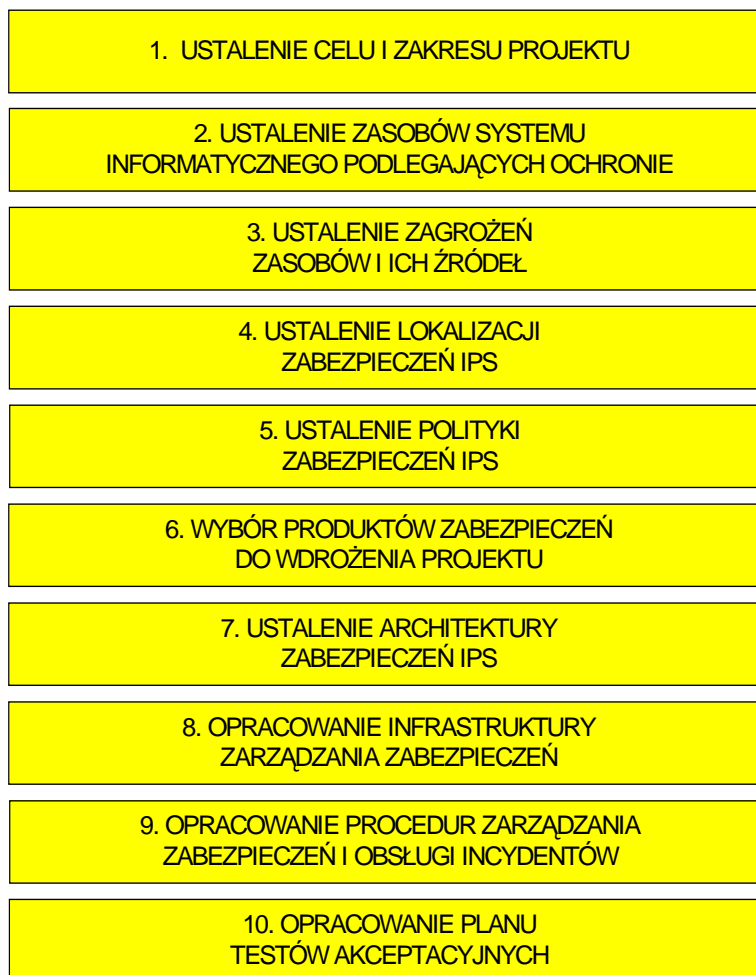


Rysunek 6. Kontrola dostępu użytkowników sieci wewnętrznej do Internetu

Z zasady „Compartmentalization of Information” wynikają poniższe szczegółowe zasady tworzenia projektu zabezpieczeń sieci:

- urządzenia i systemy komputerowe świadczące usługi w sieciach zewnętrznych (np. Internecie) powinny znajdować się w innych strefach niż urządzenia i systemy komputerowe sieci wewnętrznej (tzw. strefach DMZ),
- strategiczne zasoby systemu informatycznego powinny być zlokalizowane w dedykowanych strefach bezpieczeństwa,
- urządzenia i systemy komputerowe o niskim poziomie zaufania jak urządzenia zdalnego dostępu RAS i urządzenia dostępu sieci bezprzewodowej WLAN powinny znajdować się w dedykowanych strefach bezpieczeństwa,
- serwery świadczące usługi dla klientów i partnerów firmy powinny znajdować się w dedykowanych strefach bezpieczeństwa (tzw. strefach Ekstranet),
- stacje robocze użytkowników systemu informatycznego powinny znajdować się w innych strefach bezpieczeństwa jak serwery,
- systemy zarządzania siecią i zabezpieczeń powinny znajdować się w dedykowanych strefach bezpieczeństwa,
- systemy i urządzenia przeznaczone do prac rozwojowych powinny znajdować się w innej strefie jak systemy i urządzenia będące w eksploatacji.

Poniżej przedstawione zostały etapy tworzenia projektu zabezpieczeń Intrusion Prevention.

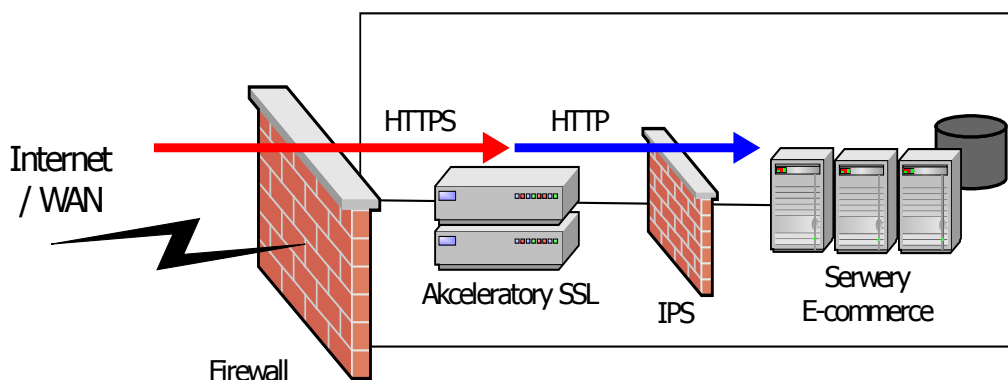


Dla skuteczności działania zabezpieczeń kluczową rolę odgrywa lokalizacja zabezpieczeń. Zabezpieczenia IPS mogą stanowić skuteczną ochronę przed atakami z sieci będąc na drodze pomiędzy chronionymi zasobami systemu informatycznego i źródłami zagrożenia (intruzami). Projektowanie zabezpieczeń w pierwszej kolejności koncentruje się na najbardziej wartościowych zasobach systemu informatycznego (tzn. systemach komputerowych realizujących, bądź wspomagających zadania biznesowe instytucji). Nie należy jednak ograniczać się tylko do ochrony najbardziej wartościowych zasobów. Projektowane zabezpieczenia sieci powinny bowiem stanowić skuteczną ochronę przed atakami prowadzonymi techniką *Island Hopping Attack*. Technika ta polega na zdobywaniu nieupoważnionego dostępu do słabiej zabezpieczonych systemów komputerowych (najczęściej nie posiadających dużego znaczenia dla instytucji), a następnie wykorzystywaniu ich jako podłoża do penetracji lepiej ochronianych, wartościowych elementów systemu informatycznego.

Identyfikacja istotnych zagrożeń systemu informatycznego wykonywana jest na podstawie analizy, m.in.:

- sposobu połączenia systemu z sieciami zewnętrznymi,
- dostępnych protokołów i usług sieci zewnętrznych,
- protokołów i usług świadczonych dla sieci zewnętrznych,
- metod współdziałania systemów zlokalizowanych w obszarach sieci o różnym poziomie zaufania (np. strefy DMZ i sieci wewnętrznej).

Projektując zabezpieczenia IPS należy także uwzględnić zagrożenie wykonywania ataków poprzez sesje szyfrowane (np. sesje HTTPS w systemach e-commerce i e-banking). Zabezpieczenia sieciowe nie są w stanie poddawać kontroli tych sesji. Skuteczną metodą ochrony jest terminowanie sesji SSL i wykonywanie kontroli na odszyfrowanych pakietach. Wdrożenie zabezpieczeń IPS dla sesji szyfrowanych wymaga zastosowania urządzeń określanych jako SSL Accelerator. Technicznie sesje HTTPS można także deszyfrować na urządzeniach IPS po skopiowaniu tam kluczy prywatnych SSL, jednak z uwagi na bezpieczeństwo materiału kryptograficznego zalecane jest wykonywanie tej operacji na specjalizowanych urządzeniach.

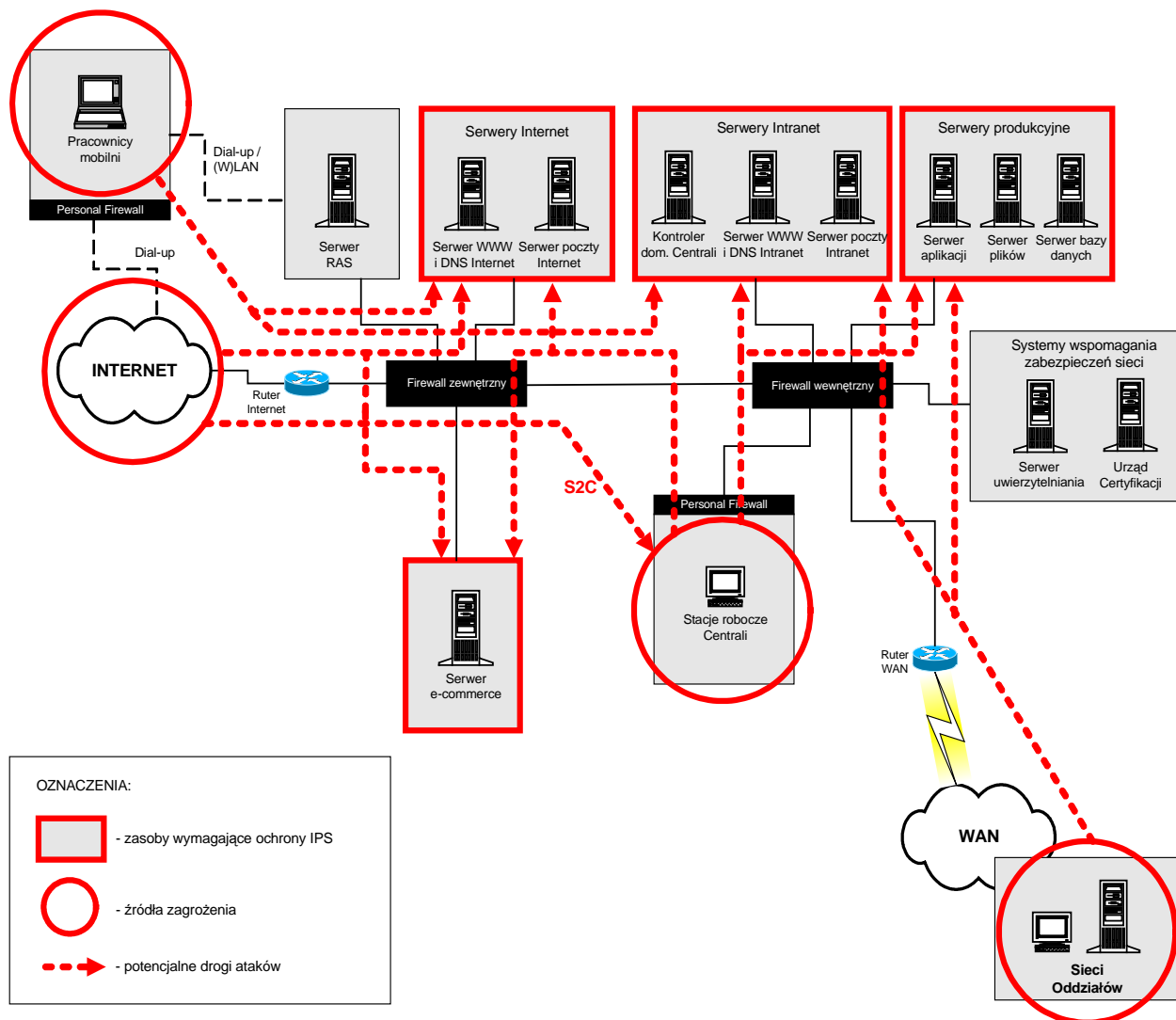


Rysunek 7. Koncepcja ochrony systemu e-commerce przed atakami poprzez SSL

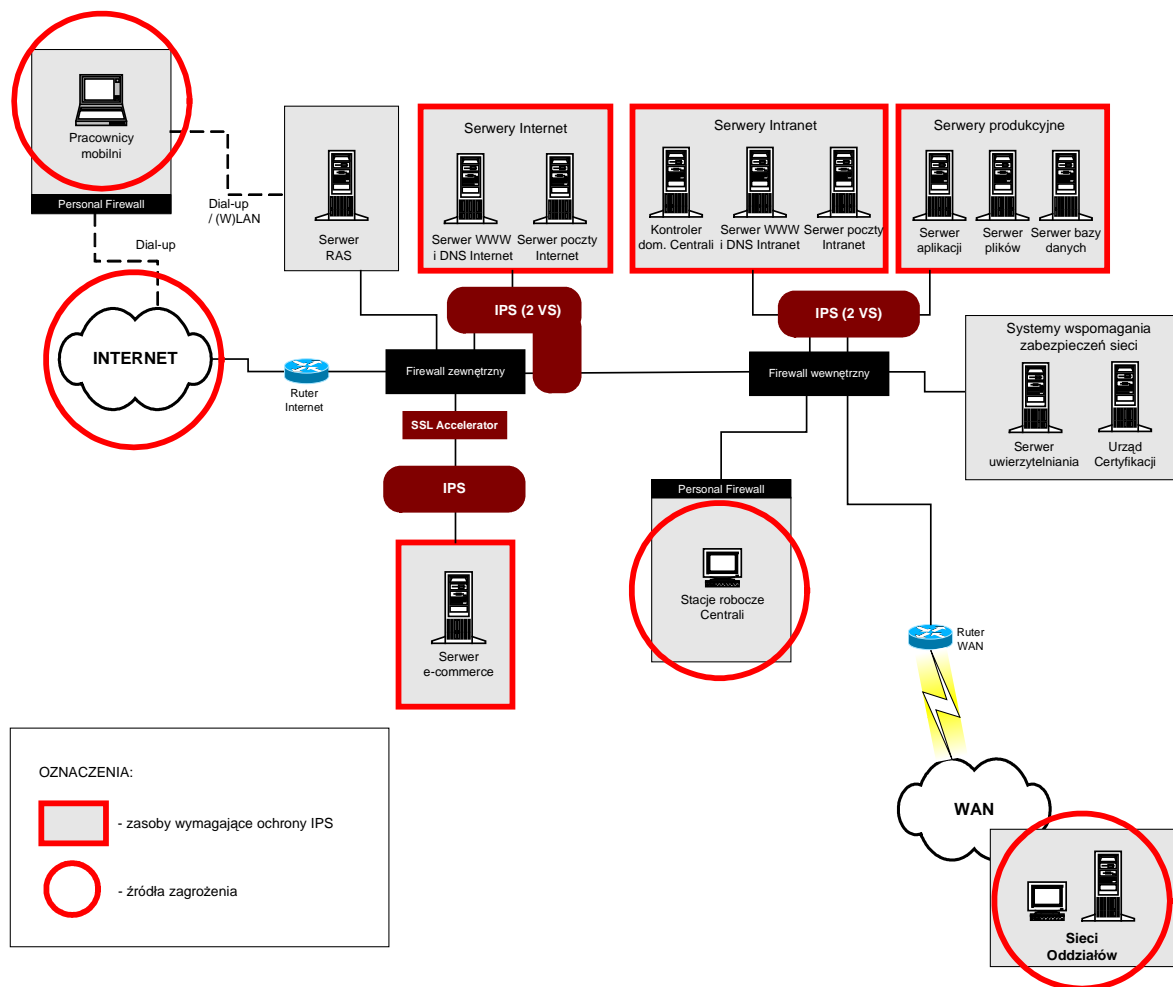
Ustalając wymagania bezpieczeństwa dla zasobów systemu informatycznego należy wziąć pod uwagę, czy są to zasoby typu „mission-critical”, gdzie priorytetem jest ciągłość działania, czy też są to zasoby „data-sensitive”, gdzie najważniejsze jest zachowanie poufności danych. Dla zasobów „mission-critical” wymagane jest zaprojektowanie zabezpieczeń IPS w konfiguracjach odpornych na awarie.

Na poniższym przykładzie przedstawione zostały kluczowe etapy projektowania zabezpieczeń IPS (patrz rysunki 8 i 9):

- ustalenie zasobów systemu informatycznego wymagających ochrony IPS,
- ustalenie zagrożeń zasobów i ich źródeł,
- ustalenie lokalizacji zabezpieczeń IPS.



Rysunek 8. Przykład projektowania zabezpieczeń IPS (etap ustalania zasobów podlegających ochronie oraz identyfikacji zagrożeń i ich źródeł)

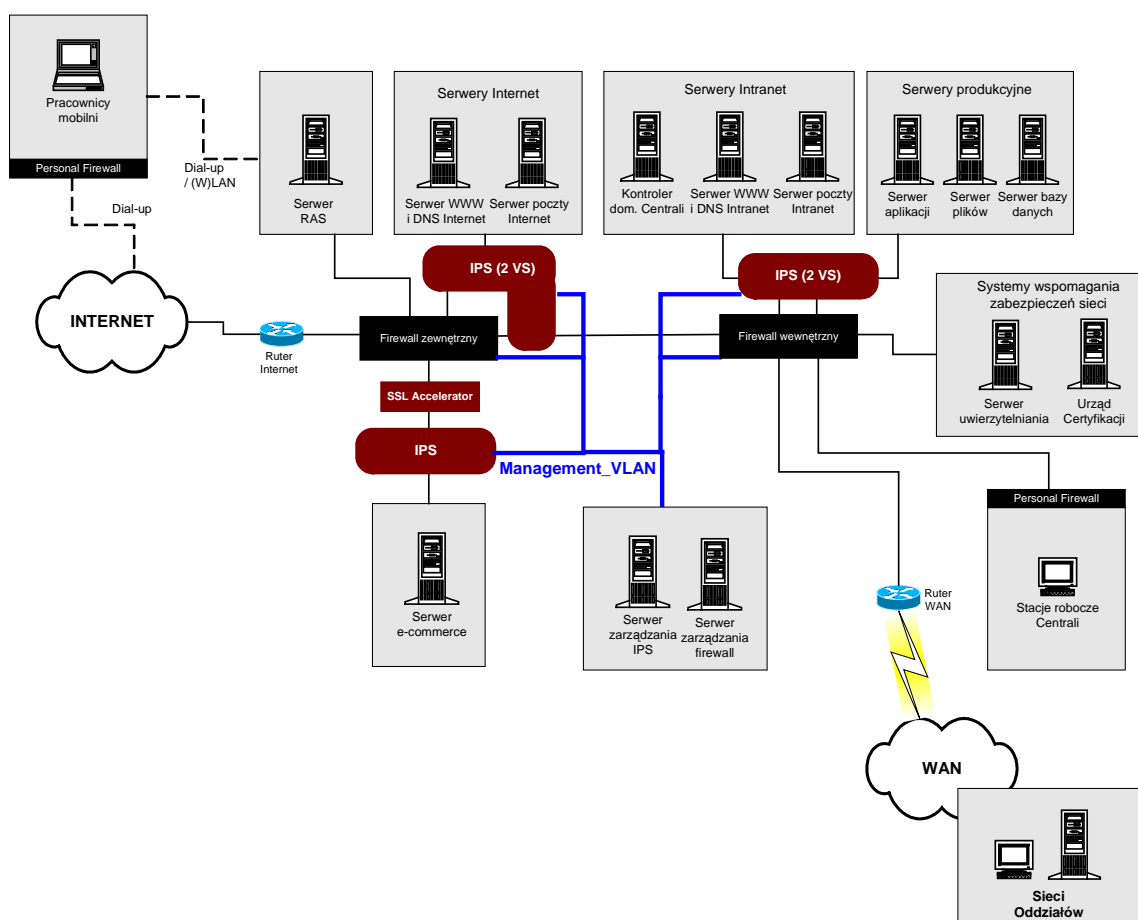


Rysunek 9. Przykład projektowania zabezpieczeń IPS (etap ustalania lokalizacji zabezpieczeń)

Wykrywanie i reagowanie na incydenty związane z naruszeniami bezpieczeństwa (m.in. sytuacje przełamania zabezpieczeń) to zagadnienia, które należy uwzględnić w projekcie zabezpieczeń. W rzeczywistości nie istnieją zabezpieczenia o stuprocentowej skuteczności i z sytuacją wtargnięcia do sieci intruza, czy robaka należy się liczyć. Włamanie może nastąpić np. z wykorzystaniem nie opublikowanego błędu bezpieczeństwa (tzw. zero-day exploit) lub od wewnątrz sieci z pominięciem zabezpieczeń IPS. Zagadnienia te należy przeanalizować w odniesieniu do chronionych zasobów systemu informatycznego oraz przewidzianych do wdrożenia zabezpieczeń (dostępnych w nich narzędzi zarządzania bezpieczeństwem) i zapisać w procedurze obsługi incydentów.

4. Opracowanie infrastruktury zarządzania zabezpieczeń

Zakres zarządzania zabezpieczeń sieciowych obejmuje czynności związane z konfiguracją (m.in. ustawienia parametrów urządzeń, tworzenie polityk), monitorowaniem pracy zabezpieczeń i diagnozowaniem problemów, a także odczytem, raportowaniem i analizą rejestrowanych zdarzeń (logów, alarmów) oraz wyjaśnianiem incydentów bezpieczeństwa. Obsługa i nadzór systemu zabezpieczeń IPS w warunkach normalnej pracy systemu powinny odbywać się z centralnego systemu zarządzania, zlokalizowanego w chronionej przez firewall strefie sieci (tzw. „Management VLAN”). Rysunek 10 przedstawia przykładowy projekt zabezpieczeń IPS wraz z systemem zarządzania. W systemach o podwyższonych wymaganiach bezpieczeństwa należy dodatkowo zadbać o wydajność i niezawodność zarządzania (m.in. redundancję stacji zarządzającej, zapasowe kanały sterowania).



Rysunek 10. Przykład projektowania zabezpieczeń IPS (etap opracowania infrastruktury zarządzania zabezpieczeń)

5. Ustalenie polityki zabezpieczeń IPS

Polityka zabezpieczeń IPS określa w jaki sposób poszczególne urządzenia zabezpieczeń powinny wykonywać zadania monitorowania i ochrony zasobów systemu informatycznego. Polityka powinna określać, m.in.:

- ruch sieciowy podlegający ochronie,
- reakcje zabezpieczeń na ataki,
- sposób powiadamiania administratorów.

Forma polityki zabezpieczeń IPS jest uzależniona od produktu wybranego do wdrożenia projektu. Poniżej przedstawiony został przykład planowania polityki zabezpieczeń dla systemu IDP. Polityka IDP składa się reguł określających jaki ruch podlega kontroli (m.in. kto jest klientem i serwerem aplikacji), jakie ataki będą w tej komunikacji wykrywane, jaka będzie reakcja zabezpieczeń i sposób powiadomienia o zdarzeniu administratorów oraz na którym urządzeniu IDP obowiązuje ta reguła polityki zabezpieczeń. Dodatkowo w regułach IDP ustalane jest, czy określona reguła kończy kontrolę komunikacji, czy też sprawdzone zostaną kolejne reguły polityki. Więcej informacji na ten temat można znaleźć w dokumentacji produktu [6].

	No.	Match		Look For	Action	Notification
		Source	Destination	Terminate Match		
reguły o szerokim zakresie kontroli	1	any	any	<input type="checkbox"/>	SCAN	None Logging Alert Log Packets(5/5)
	2	any	any	<input type="checkbox"/>	DDOS DOS	Drop Packet Logging Alert
precyzyjne reguły kontroli	3	any	SERWER_WEB	<input type="checkbox"/>	HTTP - Critical HTTP - Major	Drop Connection Logging Alert Log Packets(5/0)
	4	any	SERWER_WEB	<input checked="" type="checkbox"/>	HTTP - Minor	None Logging
	5	any	SERWER_DNS	<input type="checkbox"/>	DNS - Critical DNS - Major	Drop Connection Logging Alert Log Packets(5/0)
reguła clean-up	6	any	SERWER_DNS	<input checked="" type="checkbox"/>	DNS - Minor	None Logging
	7	any	any	<input checked="" type="checkbox"/>	Critical Major	Drop Connection Logging Alert

Rysunek 11. Polityka zabezpieczeń IPS na przykładzie Juniper Networks IDP

Reguły polityki zabezpieczeń IDP mogą posiadać szeroki zakres kontroli lub szczegółowo określać jaka komunikacja w sieci będzie kontrolowana. Reguły o szerokim zakresie kontroli nie precyzują monitorowanej komunikacji (tzn. pola „Source” i „Destination” przyjmują wartość „Any”). Powoduje to większe obciążenie urządzeń zabezpieczeń oraz możliwość generowania zdarzeń nieistotnych dla administratorów zabezpieczeń. Szczegółowe reguły IDP ustalają jaka komunikacja jest kontrolowana i jakie ataki są w niej wykrywane. Zasadniczo zalecane jest stosowanie szczegółowych reguł polityki zabezpieczeń. Należy jednak zdawać sobie sprawę z tego, że stosując szczegółowe reguły łatwiej można popełnić błędy (np. nie wskazać wszystkich chronionych zasobów) i w konsekwencji ataki mogą nie zostać zauważone. Ważne jest wtedy wprowadzenie jako ostatniej tzw. reguły czyszczącej (*ang. clean-up rule*), poddającej analizie ruch sieciowy nie określony przez wcześniejsze reguły.

Reakcja zabezpieczeń IDP na określone zdarzenia jest uzależniona od wielu czynników (m.in. wymagań dostępności chronionych zasobów, lokalizacji komputera który zainicjował zdarzenie, wielkości zagrożenia). Z reguły ataki o wysokim poziomie zagrożenia inicjowane z sieci zewnętrznych na zasoby typu „data-sensitive” powinny być blokowane. Alarmowanie bez blokowania ataków może być stosowane przy ochronie zasobów typu „mission-critical”, bądź też dla ataków inicjowanych w sieciach lokalnych, gdzie administratorzy mają kontrolę nad użytkownikami. Praca w trybie monitorowania jest także zalecana w początkowym okresie wdrożenia zabezpieczeń (tzn. w trakcie dostrajania polityki). W zakresie powiadamiania administratorów o wystąpieniu zdarzenia system zabezpieczeń IDP umożliwia zapisanie informacji w logu, wyświetlenie zdarzenia jako alarmu, zapisanie określonej liczby pakietów przed i po wystąpieniem zdarzenia (np. w celu dokładnego przeanalizowania ruchu sieciowego), wysłanie komunikatu poprzez SNMP Trap, Syslog i Email, a także uruchomienie wskazanego skryptu lub aplikacji.

W rozwiązaniu IDP polityka zabezpieczeń oprócz ochrony przed typowymi atakami z sieci (exploit, DoS) może zawierać także inne stosowane w zależności od potrzeb mechanizmy ochrony, m.in.:

- wykrywanie skanowania i prób penetracji (techniki Traffic Anomaly, zdarzenia Network Scanner Identification),
- utrudnianie skanowania i rozpoznawania systemów (mechanizm Network Honeypot),
- wykrywanie i blokowanie połączeń z aplikacjami Trojan/Backdoor (mechanizm Backdoor Detection),
- wykrywanie sytuacji „przełamania zabezpieczeń” (np. nowo otwartych portów na serwerach za pomocą mechanizmu Profiler),
- blokowanie pakietów z niewłaściwą adresacją IP i MAC (mechanizm Anti-Spoofing),
- blokowanie Spyware, Keylogger i innych złośliwych aplikacji (ataki typu Server-to-Client),
- wykrywanie nieupoważnionych komputerów podłączonych do sieci wewnętrznej (mechanizm Profiler),
- nadzorowanie przestrzegania przez pracowników przyjętej polityki bezpieczeństwa (mechanizm Profiler),
- wspomaganie administratorów w zakresie wykrywania systemów i aplikacji podatnych na błędy bezpieczeństwa (mechanizm Profiler).

Z punktu widzenia wczesnego wykrywania incydentów istotne jest wdrożenie w systemie zabezpieczeń IDP mechanizmów identyfikacji technik rekonesansu. Przed wykonaniem ataków intruzi zwykle dokonują rozpoznania obiektów ataku tak, aby dobrać odpowiednie narzędzia. Włączenie w IDP mechanizmu Network Honeypot ma na celu przekazywanie intruzom nieprawdziwych informacji nt. dostępnych usług systemu (zwykle przedstawianie usług specyficznych dla innej klasy systemów) oraz pokazywanie nieistniejących w rzeczywistości serwerów. W razie zastosowania tego mechanizmu intruz otrzymuje wiele nieprawdziwych informacji utrudniających prowadzenie dalszego ataku (np. na serwerze MS Windows zostają rozpoznane usługi specyficzne dla serwerów Unix). Znacznie utrudnione jest także rozpoznawanie systemów operacyjnych za pomocą technik TCP/IP Fingerprint. Dodatkowo włączenie w polityce zabezpieczeń IDP kategorii ataków Network Scanner Identification umożliwia wykrywanie narzędzi wykorzystanych przez intruzów do skanowania i penetracji (np. Nessus, NMAP).

W przypadku przeprowadzenia udanego włamania do systemu i zainstalowania Backdoor intruz bez wykonywania ataków może uzyskiwać do niego nieupoważniony dostęp. W systemie zabezpieczeń IDP występują dwie metody przeciwdziałania takim sytuacjom. Włączenie mechanizmu Protocol Anomaly Detection dla chronionych zasobów systemu informatycznego (tzn. w regułach polityki zabezpieczeń dodajemy odpowiednie kategorie Protocol Anomaly) powoduje, że ruch sieciowy sprawdzany jest pod kątem zgodności z obowiązującymi standardami dla poszczególnych protokołów. Dodatkowo należy skonfigurować mechanizm Backdoor Detection, który poprzez analizę heurystyczną wykrywa specyficzną dla Backdoor interakcyjną komunikację

W razie wykrycia ataku na strategiczne zasoby systemu informatycznego IDP może na określony czas całkowicie zablokować dostęp dla adresów IP, z których został wykonany atak. Ustawienia te powinny jednak zostać dobrze przemyślane przed ich zastosowaniem. Jest to bardzo „mocny” mechanizm w rękach administratora, którego zastosowanie należy odpowiednio zaplanować. Przede wszystkim nie należy stosować tego mechanizmu jako reakcji na ataki, które mogą potencjalnie być wykonane z innych adresów IP (np. ataki wykorzystujące IP Spoofing do fałszowania adresów, z których są wysyłane).

Oprócz włączenia odpowiednich mechanizmów ochrony przed atakami należy także zwrócić uwagę na właściwe dostrojenie konfiguracji zabezpieczeń IDP tak, aby uwzględniała ona specyficzne uwarunkowania systemu informatycznego, m.in. zdefiniowanie nowych ataków i zdarzeń (np. blokowanie specyficznych dla danego kraju aplikacji P2P), a także ochronę serwisów na niestandardowych portach (tzn. zdefiniowanie nowych serwisów i dodanie ich do odpowiednich reguł polityki zabezpieczeń). Ważna dla właściwego zarządzania zabezpieczeń IDP jest zredukowanie fałszywych alarmów (*ang. false positive*) oraz zdarzeń mało istotnych dla bezpieczeństwa systemu informatycznego. Odbyna się to poprzez analizę rejestrowanych logów i alarmów oraz odpowiednie dostrajanie treści reguł polityki zabezpieczeń (m.in. usuwanie z reguł zbędnych definicji ataków). Dla systemu zabezpieczeń IDP zalecenia w tym zakresie można znaleźć w dokumencie [5].

6. Projektowanie skalowanych i niezawodnych zabezpieczeń IPS

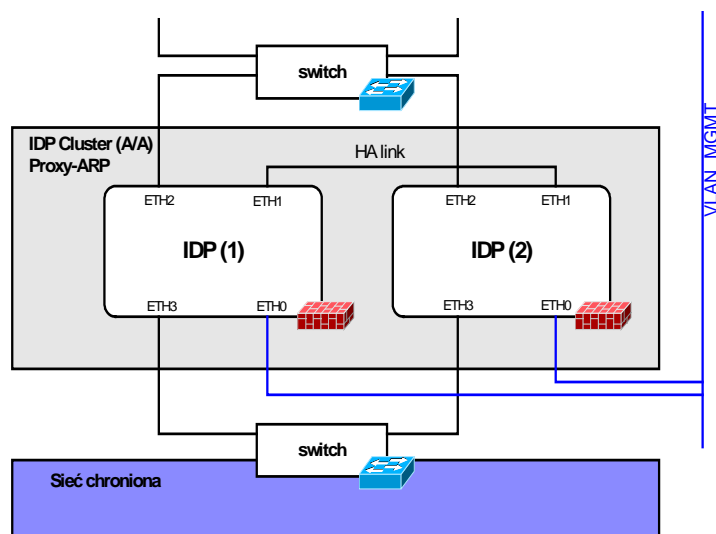
Skalowalność zabezpieczeń IPS oznacza możliwość dodania kolejnych punktów ochrony oraz podwyższenia wydajności i niezawodności istniejących zabezpieczeń bez konieczności przebudowy struktury sieci i zabezpieczeń. Projekt zabezpieczeń powinien zapewniać łatwość rozbudowy systemu zabezpieczeń o nowe elementy i mechanizmy ochrony w zakresie wielkości (dodatkowe punkty ochrony), wydajności (wyższa przepustowość łączy i intensywność ruchu) oraz niezawodności (konfiguracje redundancyjne). W trakcie wyboru produktu zabezpieczeń do wdrożenia projektu zalecane jest wybranie rozwiązania IPS zapewniającego elastyczność zabezpieczeń tzn. możliwość dopasowywania zabezpieczeń do zmieniających się warunków sieci i systemów informatycznych.

Dostępność usług systemu informatycznego funkcjonującego w środowisku sieciowym zależy od wielu różnych czynników (np. urządzeń sieciowych, łączy transmisyjnych, systemów zabezpieczeń). Z uwagi na specyfikę tego środowiska szczególnie istotnym elementem mającym wpływ na dostępność systemu są środki bezpieczeństwa zastosowane do ochrony serwerów usług przed niepożądanym działaniem złośliwych użytkowników. Podstawowym elementem zabezpieczeń sieciowych odpowiedzialnym za odpieranie tego typu ataków jest system IPS. Ważne jest więc, aby także IPS posiadał środki zabezpieczające go przed awariami sprzętowymi i programowymi. Konfiguracje zawierające mechanizmy ochrony przed awariami określane są terminem HA (*ang. high availability*).

Występują dwie podstawowe architektury (kategorie) systemów HA:

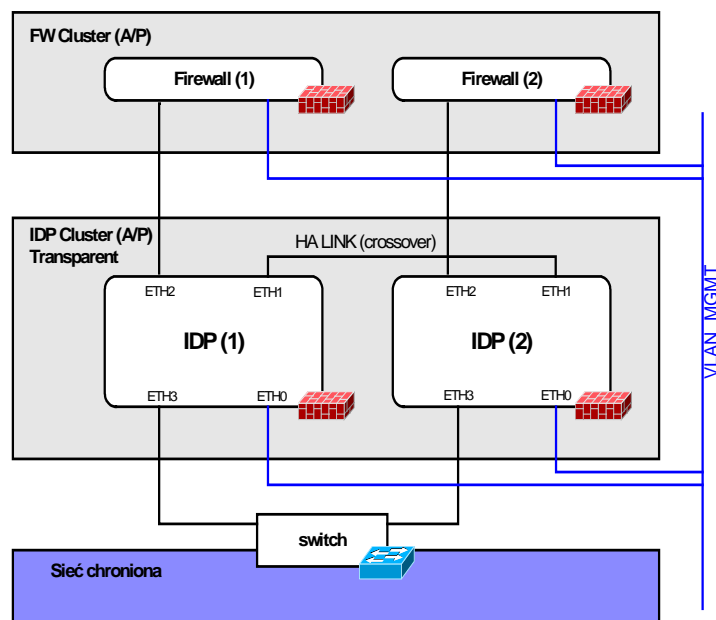
- Active-Passive (określana także jako Hot-Standby) – konfiguracja składa się z dwóch lub więcej maszyn IPS, wśród których tylko jedna jest aktywna, a pozostałe to maszyny zapasowe uruchamiane w razie awarii aktywnego IPS,
- Active-Active – konfiguracja składa się z dwóch lub więcej maszyn IPS, spiętych w klastry, współdzielących pomiędzy sobą obciążenie.

Zagadnienia projektowania konfiguracji HA zostaną omówione na przykładzie rozwiązania IDP. System zabezpieczeń IDP umożliwia wdrożenie różnych konfiguracji HA, funkcjonujących na poziomie warstwy 2 i 3 OSI. Przedstawione zostaną wybrane konfiguracje klastrowe. Konfiguracja typowego klastra IDP została przedstawiona na rysunku 12. Urządzenia zabezpieczeń funkcjonują w trybie L3 (Proxy-ARP lub Router). Projektując system zabezpieczeń IDP w takiej konfiguracji należy zapewnić, aby podłączone do klastra przełączniki sieciowe poprawnie obsługiwały multicast-owe adresy MAC. Przełącznik przesyła bowiem całość nadchodzącego ruchu do wszystkich urządzeń w klastrze HA. Urządzenia IDP komunikują się pomiędzy sobą za pomocą protokołu Heartbeat i decydują, które z nich będzie obsługiwało napływające sesje. Połączenie do synchronizacji klastra (HA link) powinno zostać zapewnione na poziomie L2 OSI. Przedstawiony na rysunku klastry HA może funkcjonować w trybach Active-Active lub Active-Passive.



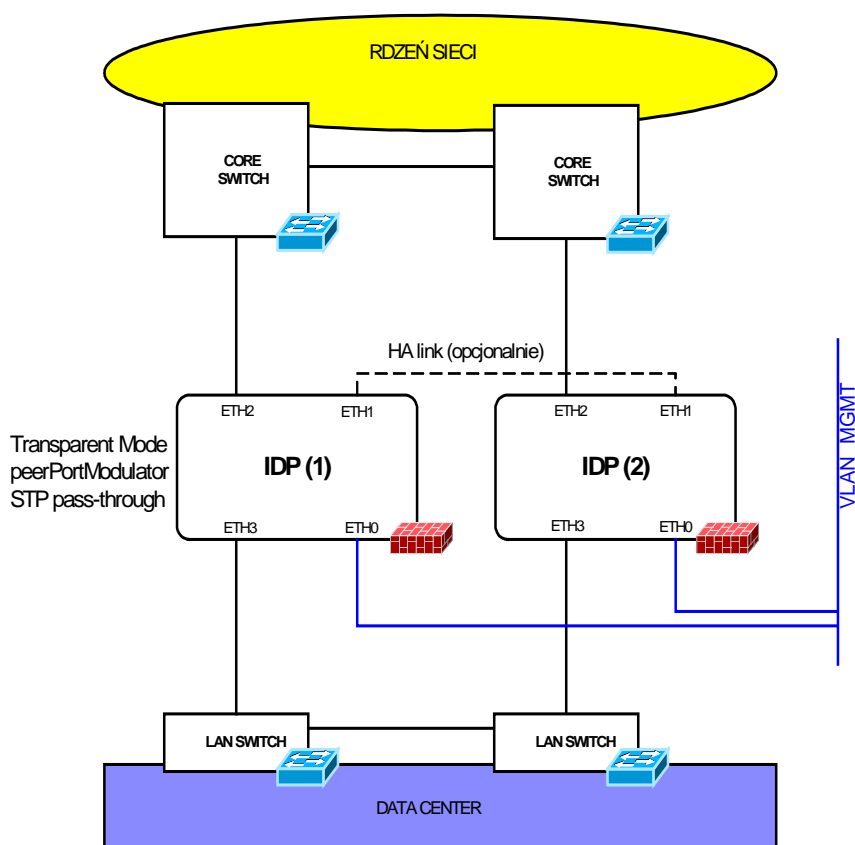
Rysunek 12. Klaster urządzeń zabezpieczeń IDP typu Active-Active

W sytuacji gdy zabezpieczenia IDP zostaną wdrożone jako uzupełnienie zabezpieczeń firewall działających w trybie klastra Active-Passive, urządzenia IDP można podłączyć w trybie transparentnym bezpośrednio za urządzeniami firewall. Taka konfiguracja została przedstawiona na rysunku 13.



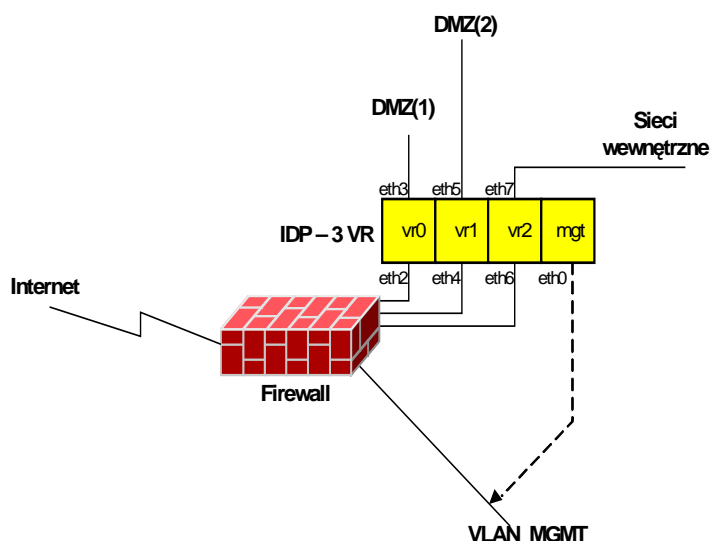
Rysunek 13. Klaster urządzeń zabezpieczeń IDP typu Active-Passive

Kontrolowanie komunikacji pomiędzy przełącznikami rdzeniowymi i dostępowymi posiada specyficzne wymagania. Najczęściej łącza te służą do przenoszenia sieci VLAN (tzn. są to łącza VLAN Trunk). W sytuacji gdy urządzenie IDP działa na podobnej zasadzie jak przełącznik sieciowy (tryb Bridge) wymagane jest odpowiednie skonfigurowanie na IDP protokołu STP, a także interfejsów VLAN oraz dla każdego z nich wirtualnych modułów zabezpieczeń VR. Może to być uciążliwe w trakcie eksploatacji zabezpieczeń. Do takich zastosowań bardziej odpowiednie są IDP działające w trybie transparentnym, gdzie ruch sieciowy poddawany jest kontroli bez względu na to czy jest tag-owany (VLAN). W przypadku gdy pomiędzy przełącznikami znajduje się łącze trunk-owe nie ma potrzeby konfigurowania na urządzeniach IDP interfejsów VLAN i IP. Urządzenia IDP mogą przy tym przepuszczać protokoły inne niż IP, umożliwiając poprawną komunikację przełączników (np. STP, Rapid STP) oraz wykrywanie awarii łącza i urządzeń. Poprzez mechanizm peerPortModulator monitorowany jest stan linków podłączonych do IDP, a w razie awarii zamykane są wszystkie interfejsy inspekcyjne urządzenia IDP należące do VR, gdzie zauważona została awaria łącza. Ma to na celu szybkie powiadomienie o awarii urządzeń sieciowych w otoczeniu IDP.

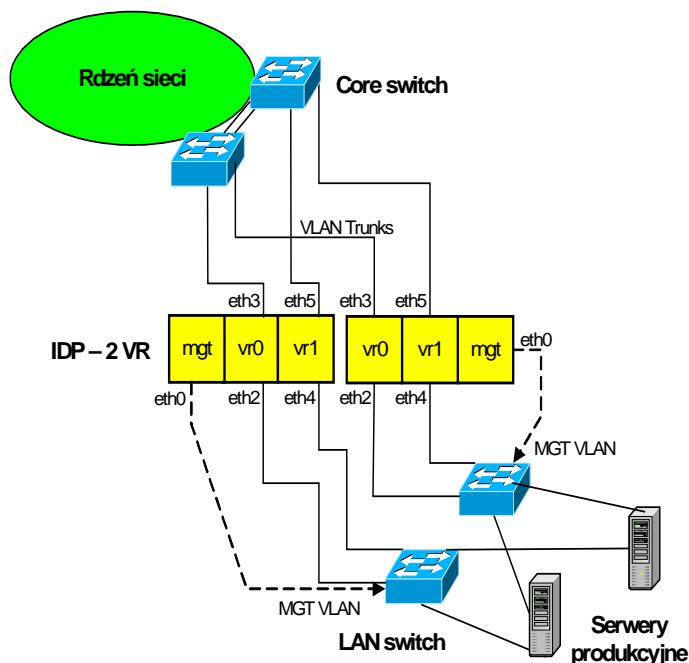


Rysunek 14. Klaster urządzeń zabezpieczeń IDP w trybie przezroczystym

Utrzymanie wysokiego poziomu bezpieczeństwa zasobów systemu informatycznego przed zagrożeniami z sieci i jednocześnie zapewnienie efektywności kosztowej jest możliwe poprzez uruchomienie na jednym fizycznym urządzeniu IPS wielu wirtualnych modułów zabezpieczeń (w rozwiązaniu IDP wirtualne moduły IPS określane są jako wirtualne routery VR). Działające w jednym urządzeniu zabezpieczeń moduły VR są odseparowane od siebie i mogą bezpiecznie kontrolować różne segmenty sieci. Na rysunkach 15 i 16 przedstawione zostały przykładowe zastosowania wirtualnych modułów zabezpieczeń w urządzeniach IDP.



Rysunek 15. Zastosowanie wirtualnych IPS do ochrony łącza z Internetem



Rysunek 16. Zastosowanie wirtualnych IPS do ochrony farmy serwerów

7. Obsługa incydentów bezpieczeństwa

Zabezpieczenia systemu informatycznego powinny być przygotowane na sytuacje wystąpienia naruszeń bezpieczeństwa. Sytuacje te określane są jako incydent. Incydent to każde niekorzystne zdarzenie, które zagraża poufności, integralności lub dostępności zasobów informacyjnych, systemów informatycznych i sieci dostarczających informacje. Każde naruszenie polityki bezpieczeństwa, polityki dopuszczalnego wykorzystania lub standardowych praktyk bezpieczeństwa to incydent. Przykładami incydentów są ataki DoS, utrata rozliczalności, uszkodzenie systemu, wprowadzenie złośliwego kodu (np. wirusa, aplikacji Trojan/Backdoor) oraz nieupoważniony dostęp do systemu.

Procedury obsługi incydentów (*ang. incident response procedures*) zawierają wytyczne do przygotowania systemu do obsługi incydentów, identyfikacji incydentów, powstrzymania rozprzestrzenia się incydentów na inne systemy, likwidacji podatności, które doprowadziły do incydentu, metod odtworzenia systemu po wystąpieniu incydentu, a także analizy zdarzeń i ustalenia wniosków mających na celu uniknięcie kolejnych incydentów [3].

Nadrzędnym celem w trakcie obsługi incydentów jest utrzymanie lub odtworzenie ciągłości działania biznesu. W trakcie obsługi incydentu konieczne jest ograniczenie rozprzestrzenia się incydentu na inne systemy (*ang. incident containment*) oraz usunięcie podatności systemu i zablokowanie źródeł zagrożenia (*ang. incident eradication*). Administrator ma do dyspozycji dwie podstawowe metody obsługi incydentów: odłączenie systemu z sieci i odtworzenie jego sprawności (np. z kopii backup) lub odtwarzanie sprawności systemu bez odłączania z sieci.

Problem decyzyjny występuje w systemach o wysokich wymaganiach dla dostępności zasobów (tzw. „mission-critical systems”), których nie można odłączyć od sieci na czas wyjaśnienia incydentu i usunięcia jego skutków. W takich przypadkach za pomocą dostępnych zabezpieczeń kontroli dostępu należy ograniczyć możliwości rozprzestrzenia się incydentu na inne systemy oraz zablokować źródło ataku. Do tego celu można wykorzystać dedykowane urządzenia firewall lub moduły filtracji zawarte w innych urządzeniach (np. ruterach, IPS). Zabezpieczenia sieciowe oraz procedury zarządzania zabezpieczeń powinny być do tego celu przygotowane.

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzeniu odpowiednich osób, bądź organów. Ważne jest aby na etapie identyfikacji incydentu, który wystąpił w sieci komputerowej została ustalona lokalizacja źródła ataku (np. adres IP). Możliwe jest wtedy odseparowanie źródła zagrożenia od zasobów systemu informatycznego za pomocą dostępnych zabezpieczeń kontroli dostępu. Ustalenie rodzaju i lokalizacji ataku może zostać wykonane za pomocą systemów wykrywania intruzów (IPS/IDS).

Zaatakowany system także stanowi potencjalne źródło zagrożenia, ponieważ intruz lub złośliwy kod (np. robak) może poprzez ten system kontynuować ataki na inne zasoby systemu informatycznego. Mając na celu uniemożliwienie rozprzestrzenia się incydentu należy odseparować zaatakowany system od reszty sieci za pomocą dostępnych zabezpieczeń. W trakcie obsługi incydentów ważny jest krótki czas i precyzja reakcji.

Wybór zabezpieczeń kontroli dostępu do odseparowania źródła ataku powinien zostać dokonany z uwzględnieniem następujących zaleceń:

- źródło ataku zostanie odizolowane od zasobów systemu informatycznego, które mogą zostać z niego potencjalnie zaatakowane,
- zostaną użyte urządzenia zabezpieczenia wyposażone w funkcje IPS/IDS lub urządzenia, dla których na drodze do źródła ataku występują zabezpieczenia IPS/IDS. Z punktu widzenia wyjaśnienia całości zdarzenia ważne jest aby źródło incydentu było w dalszym ciągu monitorowane.

W celu ograniczenia rozprzestrzenienia się incydentu na inne systemy należy zaatakowany system potraktować jak potencjalne źródło zagrożenia i w razie możliwości odizolować je od reszty systemu informatycznego. Sposób postępowania jest uzależniony od wymagań polityki bezpieczeństwa względem zaatakowanego systemu. W sytuacji gdy poufność i integralność systemu są bardziej istotne od jego dostępności system może zostać odłączony z sieci i odtworzony w trybie off-line (np. z kopii backup). W sytuacji gdy ważna jest dostępność systemu i nie jest akceptowalny przestój systemu potrzebny do jego odtworzenia należy podjąć inne działania. Odseparowanie zaatakowanego systemu należy wtedy wykonać za pomocą występujących w sieci zabezpieczeń. Należy przy tym zapewnić dostęp do usług systemu dla ważnych użytkowników (np. strategicznych klientów firmy).

8. Opracowanie planu testów akceptacyjnych

Ostatnim etapem projektowania zabezpieczeń sieci jest opracowanie planu testów akceptacyjnych, które zostaną wykonane po zakończeniu instalacji i konfiguracji zabezpieczeń. Na podstawie pozytywnego wyniku zakończenia testów akceptacyjnych system zabezpieczeń może zostać oddany do eksploatacji. Zawarty w projekcie plan testów akceptacyjnych, dla każdego z nich powinien zawierać dokładny opis sposobu jego wykonania (m.in. narzędzia, parametry wejściowe) oraz oczekiwany (pozytywny) wynik testu. Testy akceptacyjne składają się z dwóch części: testy funkcjonalne oraz testy szczelności i efektywności zabezpieczeń.

Wykonanie testów funkcjonalnych ma na celu sprawdzenie, czy wszystkie chronione zasoby i usługi sieciowe są dostępne na wymaganym poziomie poprawności i jakości (QoS). Zwykle z wykorzystaniem standardowego oprogramowania użytkowego (dla poszczególnych aplikacji) należy sprawdzić poprawność i jakość funkcjonowania wszystkich usług, które zgodnie z polityką bezpieczeństwa firmy powinny być dostępne.

Testy szczelności i efektywności zabezpieczeń mają na celu dokonanie wiarygodnej oceny poziomu bezpieczeństwa sieci w zdefiniowanej w założeniach do projektu części, pod kątem szczelności i odporności na niepożądane ingerencje w działanie chronionego systemu. Weryfikacja szczelności i efektywności systemu zabezpieczeń często realizowana jest w formie testu penetracyjnego z elementami kontrolowanej symulacji włamań. Testy powinny zostać wykonane w pierwszej kolejności z wykorzystaniem popularnych technik i narzędzi hakerskich [8]. Wymagane jest do tego celu odpowiednie zabezpieczenie samego stanowiska audytora tak, aby wyniki testów nie zostały w sposób niepożądany przesłane do Internetu. Testy zabezpieczeń powinny zostać wykonane w ścisłej współpracy z administratorami testowanych systemów. Jest to szczególnie istotne w trakcie wykonywania badań odporności systemu na ataki destrukcyjne oraz symulacji włamań, a także poprawności reakcji zabezpieczeń na wykonywane ataki. Personel obsługi zabezpieczeń zaangażowany w ich realizację powinien zostać odpowiednio do tego celu przeszkolony.

Literatura

- [1] Brookshire D., "AV Diversification, Next Generation Network Defense", SANS Institute 2004.
- [2] DISA, "Infrastructure Security Technical Implementation Guide", US Defense Information Systems Agency 2003.
- [3] FCC, "Computer Security Incident Response Guide", US Federal Communications Commission 2001.
- [4] IATFF, "Information Assurance Technical Framework", IATFF 2002.
- [5] Juniper Networks, „IDP Policy Building Primer, Building Scalable Policies with Juniper IDP”, Juniper Networks 2006.
- [6] Juniper Networks, "Intrusion Detection and Prevention, Concepts & Examples Guide, Release 4.0r3", Juniper Networks 2006.
- [7] NSA, "Defense in Depth - A practical strategy for achieving Information Assurance in today's highly networked environments", NSA 2000.
- [8] Stawowski M., „Badanie zabezpieczeń sieci komputerowych”, Arskom 1999.
- [9] Stoneburner G., Hayden C., Feringa A., "Engineering Principles for Information Technology Security", NIST 2004.
- [10] Straub K.R., "Information Security Managing Risk with Defense in Depth", SANS 2003.
- [11] Zimmerman S.C., CERT Coordination Center, "Secure Infrastructure Design", CERT 2001.