Miłosz Kutyła, Jakub Ossowski,
Jan Walczak, Patryk Jankowicz

Politechnika Warszawska

Sprawozdanie z realizacji projektu bezpiecznej architektury pt. Nowe biuro

28 grudnia 2023

Spis treści

1. Wstęp

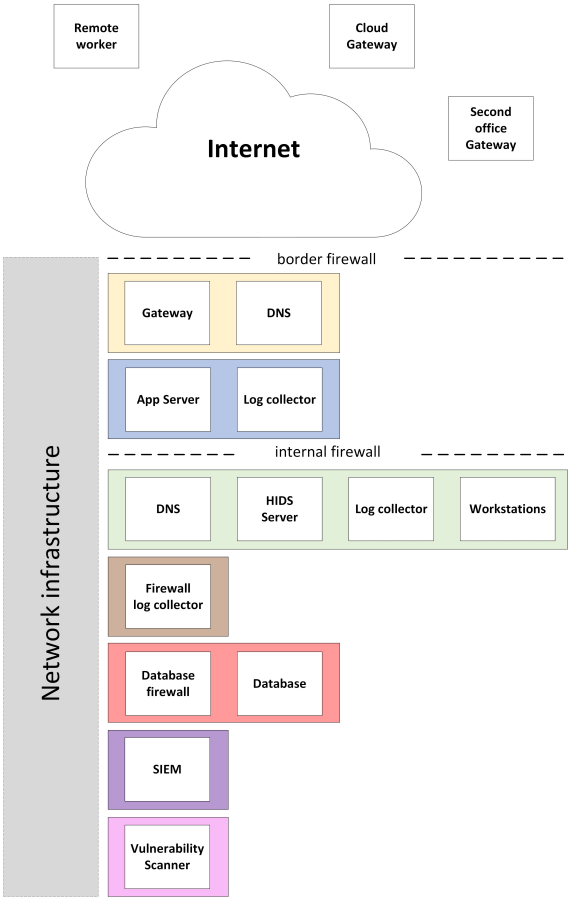
1.1. Scenariusz

Nasza firma przygotowuje się do otwarcia nowego biura. Zespół cyberbezpieczeństwa, którego jesteśmy członkami, otrzymał zadanie zaplanowania bezpiecznej architektury sieci, wykorzystując rozwiązania sieciowe i usługi bezpieczeństwa. W ramach tej sieci zaznaczone są docelowe główne obszary:

1. Główna część lokalna (najważniejsza część ćwiczenia):
   - segment żółty – stykający się z Internetem i dostępem do innych lokalizacji (patrz: obszary zdalne),
   - segment niebieski – z usługami współdzielonymi, w tym dostępnymi z Internetu (np. serwer web),
   - segment zielony – reprezentujący podstawowe środowisko pracy w biurze,
   - segment czerwony – o zaostrzonych wymaganiach dla cyberbezpieczeństwa (bardziej krytyczny).
2. Obszary zdalne: pracownik zdalny, drugie biuro firmy, cloud.

1.2. Wymagania projektowe

Docelowy projekt architektury sieci powinien uwzględnić następujące komponenty dla każdego z obszarów:



Rysunek 1: Wymagane komponenty sieci

1. Dla obszarów zewnętrznych:
   - pracownik zdalny: zdalny dostęp do stacji roboczych pierwszego biura przy pomocy host-to-site VPN,
   - drugie biuro: rozwiązanie site-to-site VPN,
   - cloud: rozwiązanie site-to-site VPN.
2. Dla obszaru lokalnego, projektowane pierwsze biuro:
   - firewall brzegowy.
   - rozwiązanie site-to-site VPN.
   - Network Intrusion Detection System (NIDS).
   - segment żółty, a w nim:
     - ◇ serwer DNS,
     - ◇ serwer przesiadkowy (jump server).
   - segment niebieski, a w nim:
     - ◇ serwer aplikacyjny,
     - ◇ kolektor logów (dla serwera DNS i NIDS).
   - firewall wewnętrzny, wydzielający strefę DMZ.
   - segment zielony (środowisko pracy), a w nim:
     - ◇ serwer DNS,
     - ◇ serwer Host Intrusion Detection System (HIDS),
     - ◇ stanowiska pracownicze z agentem HIDS,
     - ◇ kolektor logów (dla serwera DNS i HIDS).
   - segment brązowy, a w nim: kolektor logów z firewalli.
   - segment czerwony, a w nim:
     - ◇ database firewall w trybie reverse proxy,
     - ◇ baza danych z wrażliwymi informacjami.
   - segment fioletowy, a w nim Security Information and Event Management (SIEM).
   - segment różowy, a w nim skaner podatności.

2. Design wysokopoziomowy

Poszczególne segmenty wskazane w sekcji 1.2. zostaną wdrożone jako oddzielne VLANy. Systemy w ramach jednego segmentu charakteryzuje przynajmniej jedno z poniższych kryteriów:

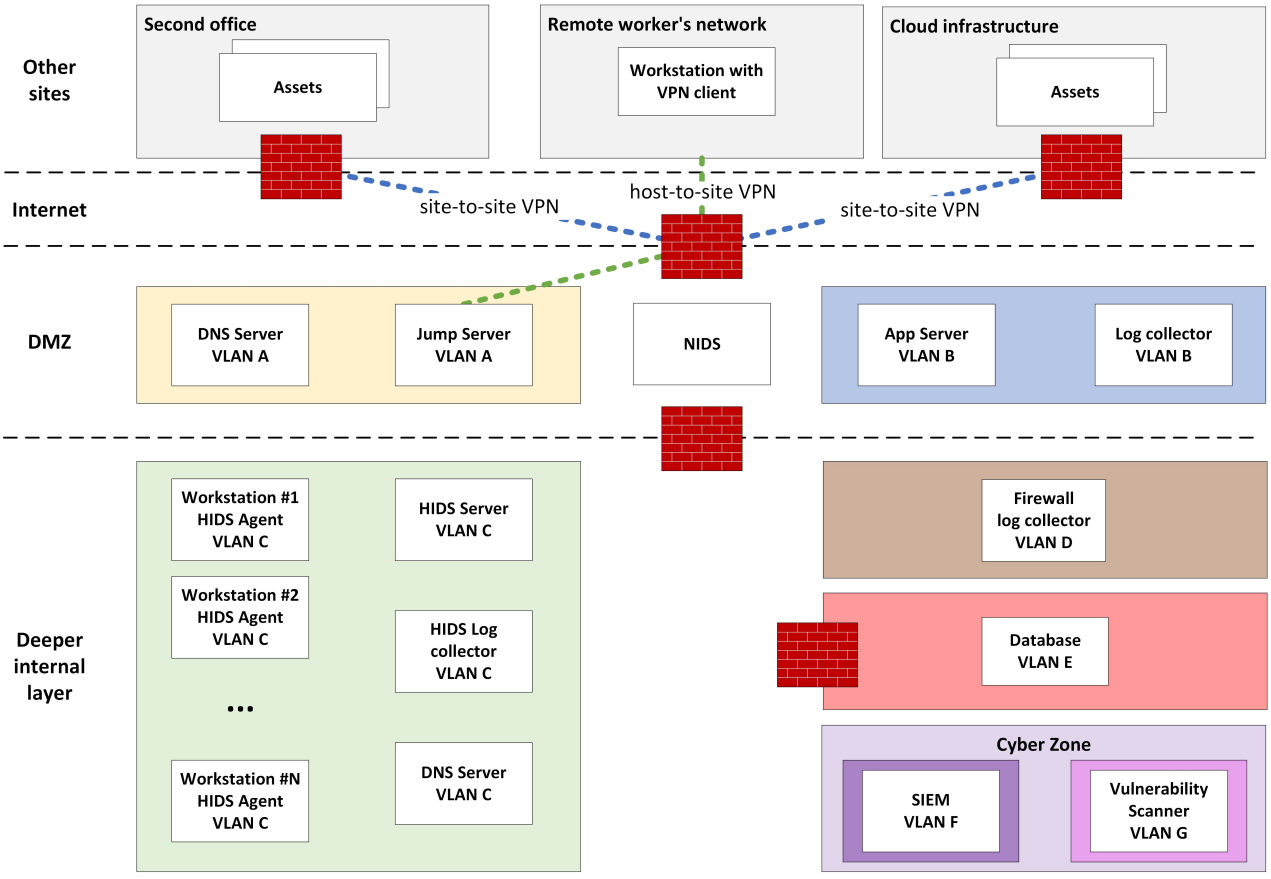
- wspólna krytyczność biznesowa systemów,
- wspólny cel biznesowy systemów,
- rozdzielenie funkcjonalności pomiędzy systemy (komplementarność, np. agent i serwer HIDS),
- ułatwienie zarządzania systemami.

Warto zaznaczyć, że podział na VLANy jest wprowadzony w celu ograniczenia ruchu broadcastowego i nie jest to bezpośrednia metoda wdrażania polityk bezpieczeństwa. Wprowadzenie VLANów jest natomiast rozwiązaniem, które ułatwia wdrażanie i stosowanie polityk bezpieczeństwa (na routerach i firewallach) dot. komunikacji między segmentami, co jest jednym z głównych celów projektowania bezpiecznych architektur. Z tego powodu wprowadzenie VLANów jest istotnym elementem projektowanej sieci.

Ze względu na podobne wymagania bezpieczeństwa dotyczące m.in. ich funkcjonalności lub konfiguracji dostępu, następujące segmenty zagregowaliśmy do stref:

- segment niebieski i segment żółty: strefa DMZ.
- segment fioletowy i segment rożowy: strefa Cyber Zone.

Zasugerowaną segmentację na schemacie wysokopoziomowym sieci przedstawia rysunek 2.

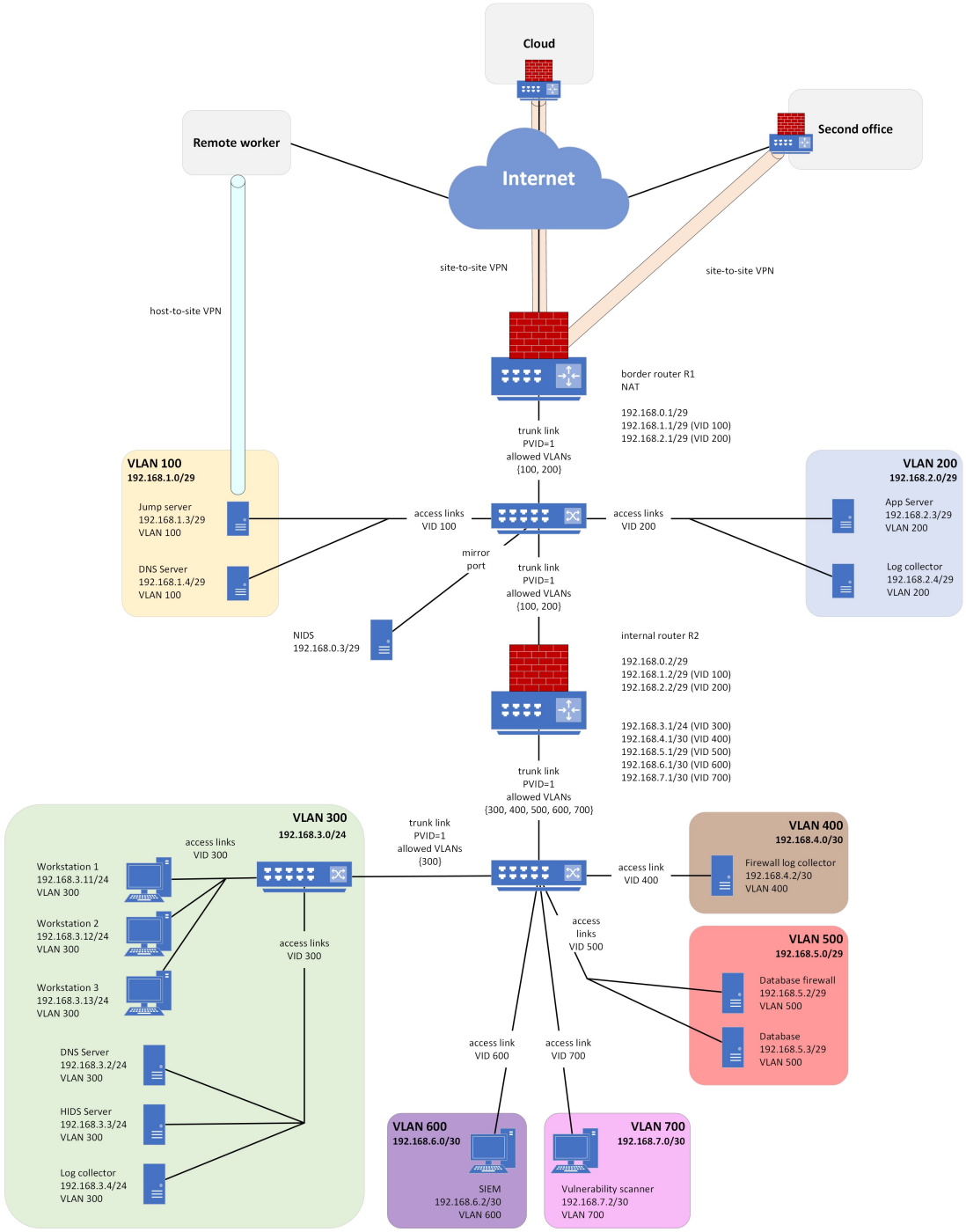


Rysunek 2: Sugerowana topologia sieci: schemat wysokopoziomowy

3. Design niskopoziomowy

W celu wstępnego zaplanowania procesu wdrażania zaprojektowanej infrastruktury, utworzyliśmy schemat niskopoziomowy sieci. Przybliża on informacje o m.in. typach połączeń między maszynami, switchami i routerami, a także o sposobie implementacji firewalli (router lub osobna maszyna), które będą odpowiadały za kontrolowanie ruchu z Internetu, do Internetu oraz w sieci wewnętrznej. Dodatkowo obrazuje on zestawiane połączenia VPN między elementami sieci projektowanego biura a obszarami zdalnymi.

Sugerowaną topologię sieci na schemacie niskopoziomowym przedstawia rysunek 3. Oznaczenia przedstawione na tym schemacie (np. router R1, router R2) są stosowane w dalszej części dokumentacji.



Rysunek 3: Sugerowana topologia sieci: schemat niskopoziomowy

4. Konfiguracja portów i usług

4.1. Usługi bezpieczeństwa

W poniższych tabelach przedstawione zostały konfiguracje otwartych portów dla poszczególnych usług bezpieczeństwa. Znak "x" oznacza jeden otwarty port, którego konkretna numeracja nie została jeszcze ustalona na tym etapie projektu.

Kolektor logów – segment niebieski	
x	Przyjmowanie logów od serwera DNS
x	Przyjmowanie logów od serwera aplikacyjnego
x	Przyjmowanie logów od NIDS
x	Wysyłanie logów do SIEM'a w strefie Cyber Zone

Tabela 1: Konfiguracja portów i usług dla kolektora logów w segmencie niebieskim

Kolektor logów – segment zielony	
x	Przyjmowanie logów od serwera DNS
x	Przyjmowanie logów od serwera HIDS
x	Wysyłanie logów do SIEM'a w strefie Cyber Zone

Tabela 2: Konfiguracja portów i usług dla kolektora logów w segmencie zielonym

Kolektor logów – segment brązowy	
x	Przyjmowanie logów od firewalla brzegowego (na routerze R1)
x	Przyjmowanie logów od firewalla wewnętrznego (na routerze R2)
x	Przyjmowanie logów od firewalla bazodanowego
x	Wysyłanie logów do SIEM'a w strefie Cyber Zone

Tabela 3: Konfiguracja portów i usług dla kolektora logów w segmencie brązowym

NIDS	
x	Odbieranie kopii ruchu ze switcha
x	Wysyłanie logów do kolektora w segmencie niebieskim

Tabela 4: Konfiguracja portów i usług dla NIDS

Serwer HIDS	
$N \cdot x$	Odbieranie logów z agentów HIDS, jeden port na jednego z N agentów
x	Wysyłanie logów do log kolektora w segmencie zielonym

Tabela 5: Konfiguracja portów i usług dla serwera HIDS

SIEM	
x	Odbieranie logów od kolektora z segmentu niebieskiego
x	Odbieranie logów od kolektora z segmentu zielonego
x	Odbieranie logów od kolektora z segmentu brązowego

Tabela 6: Konfiguracja portów i usług dla SIEM

Skaner podatności	
x	Wszystkie porty zamknięte, zezwalanie na odpowiedzi na zainicjowane połączenia

Tabela 7: Konfiguracja portów i usług dla skanera podatności

Database firewall	
x	Przyjmowanie zapytań SQL (reverse proxy)
x	Przekazywanie poprawnych zapytań SQL do serwera DB (reverse proxy)
x	Wysyłanie logów do log kolektora w segmencie brązowym

Tabela 8: Konfiguracja portów i usług dla database firewalla

4.2. Pozostałe usługi i hosty

W poniższych tabelach przedstawione zostały konfiguracje otwartych portów dla pozostałych usług i hostów znajdujących się w projektowanej przez nas sieci. Znak "x" oznacza jeden otwarty port, którego konkretna numeracja nie została jeszcze ustalona na tym etapie projektu.

Serwer DNS - segment żółty	
53	Port do obsługi zapytań DNS
x	Wysyłanie logów do log kolektora w segmencie niebieskim

Tabela 9: Konfiguracja portów i usług dla serwera DNS w segmencie żółtym

Serwer przesiadkowy (jump server)	
x	Port dla usługi VPN
x	Port do komunikacji z wybranymi hostami w segmencie zielonym

Tabela 10: Konfiguracja portów i usług dla serwera przesiadkowego

Serwer aplikacyjny	
433	Port dla obsługi żądań HTTPS
x	Wysyłanie logów do kolektora w segmencie niebieskim

Tabela 11: Konfiguracja portów i usług dla serwera aplikacyjnego

Serwer DNS - segment zielony	
53	Port do obsługi zapytań DNS
x	Wysyłanie logów do kolektora w segmencie zielonym

Tabela 12: Konfiguracja portów i usług dla serwera DNS w segmencie zielonym

Host biurowy (workstation)	
N·x	Porty do realizacji zadań biurowych przewidzianych dla danego stanowiska
x	Wysyłanie logów do serwera HIDS

Tabela 13: Konfiguracja portów i usług dla hosta biurowego

Baza danych	
5432	Port do realizacji zapytań SQL

Tabela 14: Konfiguracja portów i usług dla bazy danych

5. Wymagania bezpieczeństwa

5.1. Komunikacja między obszarami

Zaplanowaliśmy podstawową komunikację jaka może zachodzić pomiędzy poszczególnymi obszarami. Wyrażenie "TAK" oraz zielona komórka w macierzy komunikacji oznacza bezpośrednią komunikację dwustronną, podczas gdy komórka żółta oznacza ograniczoną komunikację na specjalnych zasadach opisanych wewnątrz komórki. Macierz komunikacji między wyróżnionymi przez nas obszarami przedstawia rysunek 4.

	Pracownik Zdalny	Cloud	Drugie biuro	Segment ŻÓŁTY	Segment NIEBIESKI	Segment ZIELONY	Segment CZERWONY	Segment BRĄZOWY	CYBER ZONE
Pracownik Zdalny		NIE	NIE	VPN Host-to-Site	Określone usługi	Przez jump server	NIE	NIE	NIE
Cloud	NIE		NIE	VPN Site-to-Site	NIE	NIE	NIE	NIE	NIE
Drugie biuro	NIE	NIE		VPN Site-to-Site	NIE	Przez jump server	NIE	NIE	NIE
Segment ŻÓŁTY	VPN Host-to-Site	VPN Site-to-Site	VPN Site-to-Site		TAK	Przez jump server	NIE	NIE	NIE
Segment NIEBIESKI	Określone usługi	NIE	NIE	TAK		TAK	NIE	NIE	Skan, Przekazanie logów
Segment ZIELONY	Przez jump server	NIE	Przez jump server	Przez jump server	TAK		Ograniczony dostęp (ACL)	NIE	Skan, Przekazanie logów
Segment CZERWONY	NIE	NIE	NIE	NIE	NIE	Ograniczony dostęp (ACL)		NIE	NIE
Segment BRĄZOWY	NIE	NIE	NIE	NIE	NIE	NIE	NIE		Przekazanie logów
CYBER ZONE	NIE	NIE	NIE	NIE	Skan, Przekazanie logów	Skan, Przekazanie logów	NIE	Przekazanie logów	

LEGENDA
Cały ruch sieciowy jest dozwolony
Ruch sieciowy jest częściowo dozwolony pod pewnymi warunkami
Ruch sieciowy całkowicie zabroniony
Nieaplikowalne (domyślne deny)

Rysunek 4: Macierz komunikacji pomiędzy obszarami

5.2. Konfiguracja firewalli

Zdecydowaliśmy się na umieszczenie trzech firewalli w naszej sieci: dwóch sieciowych i jeden bazodanowy. Firewalle sieciowe będą działać w trybie `deny all` i zezwalać jedynie na zdefiniowane przypadki ruchu.

5.2.1. Firewall brzegowy

Pierwszym firewallem sieciowym jest firewall brzegowy, umieszczony na routerze brzegowym R1 przed strefą DMZ. Firewall ten przepuszcza komunikację z sieci zewnętrznych do serwera przesiadkowego oraz odpowiednich oferowanych usług z segmentu niebieskiego. Zezwala również na dostęp hostów do Internetu. Macierz dopuszczalnych i blokowanych połączeń z rozróżnieniem na połączenia przychodzące oraz wychodzące została przedstawiona na rysunku 5.

DESTINATION \ SOURCE	Internet	Pracownik Zdalny	Cloud	Drugie biuro	Segment ŻÓŁTY	NIDS	Segment NIEBIESKI	Router R2 i strefa za DMZ
Internet		NIE	NIE	NIE	TAK	TAK	TAK	TAK
Pracownik Zdalny	NIE		NIE	NIE	VPN Host-to-Site	NIE	Ruch z wybranych usług	NIE
Cloud	NIE	NIE		NIE	VPN Site-to-Site	NIE	Ruch z wybranych usług	NIE
Drugie biuro	NIE	NIE	NIE		VPN Site-to-Site	NIE	Ruch z wybranych usług	NIE
Segment ŻÓŁTY	Ruch skorelowany	VPN Host-to-Site	VPN Site-to-Site	VPN Site-to-Site		NIE	NIE	NIE
NIDS	Ruch skorelowany	NIE	NIE	NIE	NIE		NIE	NIE
Segment NIEBIESKI	Ruch na wybrane usługi	Ruch na wybrane usługi	Ruch na wybrane usługi	Ruch na wybrane usługi	NIE	NIE		NIE
Router R2 i strefa za DMZ	Ruch skorelowany	NIE	NIE	NIE	NIE	NIE	NIE	

LEGENDA
Cały ruch sieciowy jest dozwolony
Ruch sieciowy jest częściowo dozwolony pod pewnymi warunkami
Ruch sieciowy całkowicie zabroniony
Nieaplikowalne (domyślne deny)

Rysunek 5: Macierz komunikacji dla firewalla brzegowego na routerze R1

5.2.2. Firewall wewnętrzny

Drugi firewall zostanie umieszczony na routerze R2 znajdującym się na granicy strefy DMZ i głębszego poziomu sieci. Firewall ten zezwala na komunikację z serwera przesiadkowego do segmentu zielonego oraz niektórych oferowanych usług z segmentu niebieskiego do segmentu zielonego. Pozwala na komunikację kolektora logów z segmentu niebieskiego z SIEM'em w strefie Cyber Zone. Dopuszcza również ruch skanera ze strefy Cyber Zone do segmentu niebieskiego oraz żółtego. Macierz dopuszczalnych i blokowanych połączeń z rozróżnieniem na połączenia przychodzące oraz wychodzące została przedstawiona na rysunku 6.

DESTINATION \ SOURCE	Internet	Border firewall (R1)	Segment ŻÓŁTY	Segment NIEBIESKI	Segment ZIELONY	Segment CZERWONY	Segment BRĄZOWY	CYBER ZONE
Internet		NIE	NIE	NIE	TAK	NIE	NIE	TAK
Border firewall (R1)	NIE		NIE	NIE	NIE	NIE	NIE	NIE
Segment ŻÓŁTY	NIE	NIE		DNS query	Ruch do jump server, DNS query	NIE	NIE	Skan
Segment NIEBIESKI	NIE	NIE	Przekazanie logów, DNS response		Ruch na wybrane usługi	NIE	NIE	Skan
Segment ZIELONY	Ruch skorelowany	NIE	Ruch z jump server, DNS response	Ruch z wybranych usług		Ograniczona komunikacja Konkretne hosty	NIE	NIE
Segment CZERWONY	NIE	NIE	NIE	NIE	Ograniczona komunikacja Konkretne hosty		NIE	NIE
Segment BRĄZOWY	NIE	Przekazanie logów	NIE	NIE	NIE	Przekazanie logów z DB FW		NIE
CYBER ZONE	Ruch skorelowany	NIE	Skan	Skan, Przekazanie logów	Przekazanie logów z HIDS	NIE	Przekazanie logów	

LEGENDA
Cały ruch sieciowy jest dozwolony
Ruch sieciowy jest częściowo dozwolony pod pewnymi warunkami
Ruch sieciowy całkowicie zabroniony
Nieaplikowalne (domyślne deny)

Rysunek 6: Macierz komunikacji dla firewalla wewnętrznego na routerze R2

5.2.3. Firewall bazodanowy

Kolejnym firewallem na jaki się zdecydowaliśmy jest database firewall (DBFW) działający w trybie reverse proxy, umieszczony wewnątrz segmentu czerwonego. Zapewni on dodatkową warstwę bezpieczeństwa dla krytycznego zasobu z segmentu czerwonego – bazy danych. Będzie kontrolował zapytania SQL i blokował te złośliwe lub nietypowe. Będzie również blokował potencjalne wycieki danych.

5.3. Skaner podatności

Wdrożenie skanera podatności jako jednego z komponentów architektury bezpieczeństwa w projektowanej przez nas sieci umożliwia przeprowadzanie regularnego, cyklicznego skanowania wybranych elementów infrastruktury. Zgodnie z założeniami, skaner ma za zadanie skanować komponenty znajdujące się w segmencie niebieskim oraz zielonym poszukując znanych podatności. Z tego powodu zarówno ruch pochodzący ze skanera i skierowany to tych segmentów, jak i ruch w przeciwnym kierunku, powinny być dozwolone na firewallu wewnętrznym. Taka konfiguracji pozwoli na jak najdokładniejsze przeskanowanie poszczególnych segmentów i enumeracji działających usług na poszczególnych hostach w celu wykrycia związanych z nimi potencjalnych

podatności. Kluczowy dla skanera jest również bieżący dostęp do Internetu umożliwiający pobieranie najnowszych aktualizacji, które są kluczowe dla jego prawidłowego działania i możliwości wykrywania najnowszych podatności.

5.4. NIDS

NIDS (Network Intrusion Detection System) służy do wykrywania anomalii w ruchu sieciowym, a w przypadku ich wystąpienia, zawiadomienia odpowiedniego podmiotu. Warto zaznaczyć, że NIDS jest wpięty równolegle i jedynie analizuje kopie ruchu sieciowego. Nie ma tym samym bezpośredniej możliwości zapobiegania atakom (np. przez odcięcie dostępu do Internetu). W zaprojektowanej sieci przyłączymy go do portu SPAN switcha w strefie zdemilitaryzowanej.

5.5. HIDS

HIDS (Host-Based Intrusion Detection System) to system detekcji anomalii na poziomie hosta. Jego głównym celem jest monitorowanie i analiza aktywności na konkretnym urządzeniu lub w jego systemie operacyjnym. W naszym rozwiązaniu monitorowanie hostów w segmencie zielonym przy pomocy HIDS zostanie zrealizowane przy pomocy:

- agentów HIDS zainstalowanych na poszczególnych urządzeniach,
- serwera HIDS, działającego na oddzielnym hoście.

Agenci mogą przesyłać do serwera informacje takie jak logi systemowe, pliki konfiguracyjne czy aktywność aplikacji działających na urządzeniu. Następnie serwer analizuje otrzymane dane i w przypadku wykrycia anomalii, generuje alert i przesyła go do kolektora logów działającego w segmencie zielonym. Warto zaznaczyć, że dla serwera HIDS kluczowy jest bieżący dostęp do Internetu umożliwiający aktualizację sygnatur. Dzięki temu serwer HIDS może skuteczniej wykrywać anomalie.

5.6. Kolektory logów i SIEM

Ostatnim elementem bezpieczeństwa w zaprojektowanej sieci jest zbieranie logów. Kolektory logów zostały umieszczone w:

- segmencie niebieskim – ten kolektor zbiera logi pochodzące z serwera DNS z segmentu żółtego, z serwera aplikacyjnego z segmentu niebieskiego oraz z NIDS.
- segmencie zielonym – ten kolektora zbiera logi z lokalnego serwera DNS oraz zdarzenia wykryte przez serwer HIDS.
- segmencie brązowym – ten kolektor zbiera logi ze wszystkich firewalli.

Ostatecznie wszystkie kolektory wysyłają zebrane logi do SIEM'a, znajdującego się w strefie Cyber Zone. SIEM umożliwia agregację, indeksowanie i przeszukiwanie logów, a także wykrywanie anomalii na podstawie definiowanych reguł.

6. Wnioski i podsumowanie

Zadanie uważamy za ciekawe w realizacji. Liczebność i różnorodność hostów oraz usług do zaimplementowania sprawiła, że proces projektowania sieci przypominał "grę w szachy" (co dobrze odzwierciedlają macierze komunikacji), której celem było jak najlepsze (najbardziej optymalne) zabezpieczenie tworzonej sieci. Kluczem do realizacji projektu na możliwie jak największym poziomie była burza mózgów przeprowadzona w pierwszych etapach projektowania. Pozwoliła nam ona na wybranie tych najbardziej odpowiadających nam pomysłów, które jednocześnie spełnią postawione wymagania. Istotny okazał się również pierwszy, roboczy diagram architektury, który stanowił bazę do dalszej pracy.

W ramach realizacji projektu wykorzystaliśmy następujące narzędzia:

- Overleaf i Latex – do utworzenia niniejszego sprawozdania.
- draw.io – do utworzenia wstępnych diagramów.
- Microsoft Visio – do utworzenia diagramów umieszczonych w sprawozdaniu.
- Microsoft Excel – do utworzenia macierzy komunikacji oraz śledzenia postępów prac.