

Miłosz Kutyła (318427), Jakub Ossowski (318435),
Jan Walczak (318456), Patryk Jankowicz (318422)

Politechnika Warszawska

Całościowa dokumentacji z realizacji
projektów i laboratoriów BEKOM nr 2 i 3

24 stycznia 2024



WOJK Security
SAFETY AMPLIFIED

Spis treści

Oświadczenie	3
I. Projekt 2.: Bezpieczne architektury sieci	
1. Wstęp	4
1.1. Scenariusz	4
1.2. Wymagania projektowe	4
2. Design wysokopoziomowy	5
3. Design niskopoziomowy	6
4. Konfiguracja portów i usług	7
4.1. Usługi bezpieczeństwa	7
4.2. Pozostałe usługi i hosty	8
5. Wymagania bezpieczeństwa	9
5.1. Komunikacja między obszarami	9
5.2. Konfiguracja firewalli	10
5.2.1. Firewall brzegowy	10
5.2.2. Firewall wewnętrzny	11
5.2.3. Firewall bazodanowy	11
5.3. Skaner podatności	11
5.4. NIDS	12
5.5. HIDS	12
5.6. Kolektory logów i SIEM	12
6. Wnioski i podsumowanie	12
II. Laboratorium 2.: Bezpieczne architektury sieci	
7. Wymagania laboratoryjne	13
8. Wybrane przez nas elementy	13
9. Topologia sieci	14
10.Konfiguracja komponentów sieci	14
10.1. Serwer aplikacyjny	14
10.2. Serwer DNS	15
10.3. Rozwiązanie SIEM	16
10.4. Segmentacja sieci	17
10.5. Firewalle	17
10.6. VPN site-to-site	19
11.Wnioski i podsumowanie	19
III. Projekt i Laboratorium 3.: Audyt bezpieczeństwa sieci	
12.Wstęp	20
13.Część aktywna	20
13.1. Testy penetracyjne aplikacji webowej	20
13.2. Testy penetracyjne infrastruktury sieciowej	21
14.Audyt względem standardu	22
15.Podsumowanie	22
IV. Załączniki	
16.Konfiguracja komponentów sieciowych (laboratorium 2)	23
16.1. Routery	23
16.1.1. Konfiguracja routera brzegowego	23
16.1.2. Konfiguracja routera wewnętrznego	24
16.1.3. Konfiguracja routera w drugim biurze	25
16.2. Switche	27
16.2.1. Konfiguracja switcha S1	27
16.2.2. Konfiguracja switcha S2	27
16.2.3. Konfiguracja switcha S3 (VLAN 300)	28
17.Tabela względem NIST CSF	28

Oświadczenie

Niniejszy dokument to sprawozdanie z realizacji projektów i laboratoriów w ramach przedmiotu BEKOM. Oświadczamy, że ta praca, stanowiąca podstawę do uznania osiągnięcia efektów uczenia się z przedmiotu BE-KOM, została wykonana przez nas samodzielnie.

Część I

Projekt 2.: Bezpieczne architektury sieci

1. Wstęp

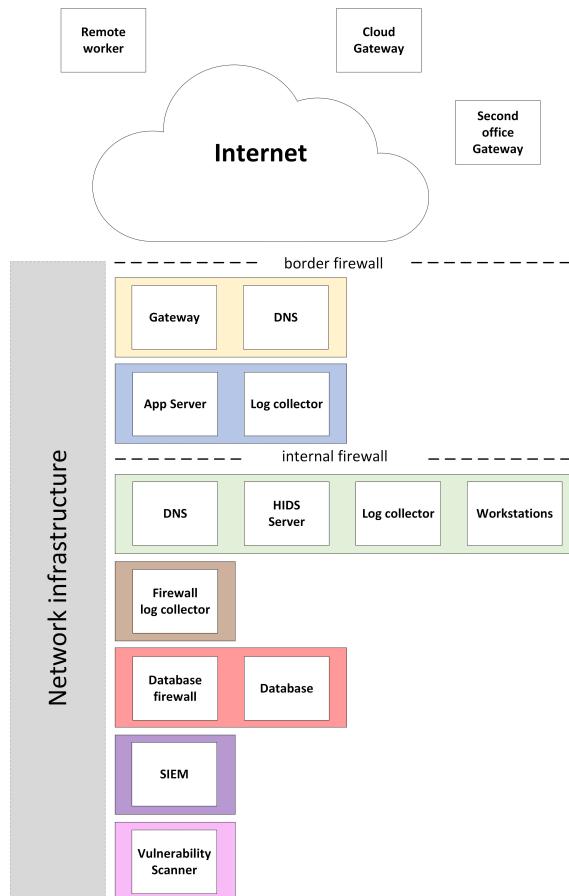
1.1. Scenariusz

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:



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.

Rysunek 1: Wymagane komponenty sieci

2. Design wysokopoziomowy

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

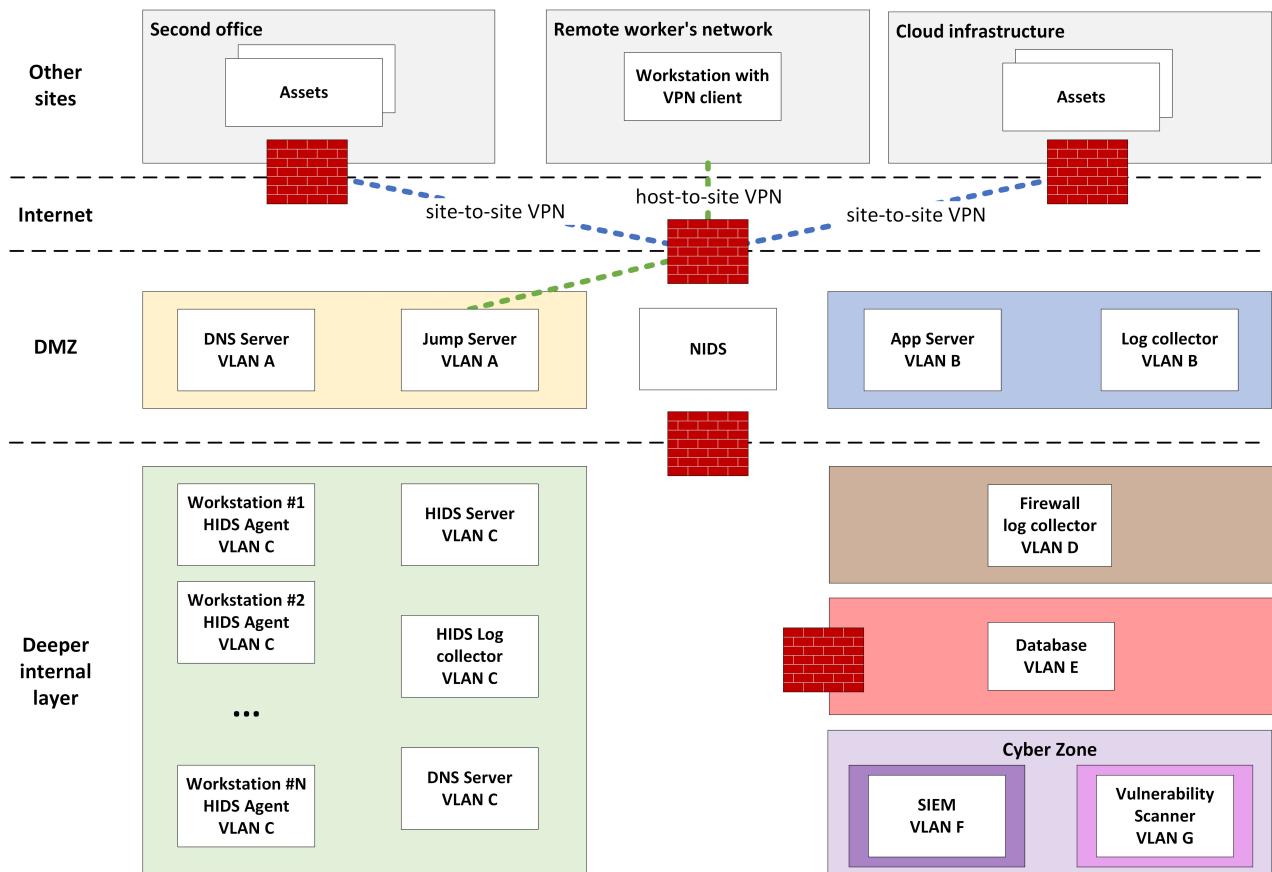
- wspólna krytyczność biznesowa systemów,
- wspólny cel biznesowy systemów,
- rozdzielenie funkcjonalności pomiędzy systemy (komplementarność, np. agent i serwer HIDS),
- ułatwienie zarządzania systemami.

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 różowy: strefa Cyber Zone.

Zasugerowaną segmentację na schemacie wysokopoziomowym sieci przedstawia rysunek 2.

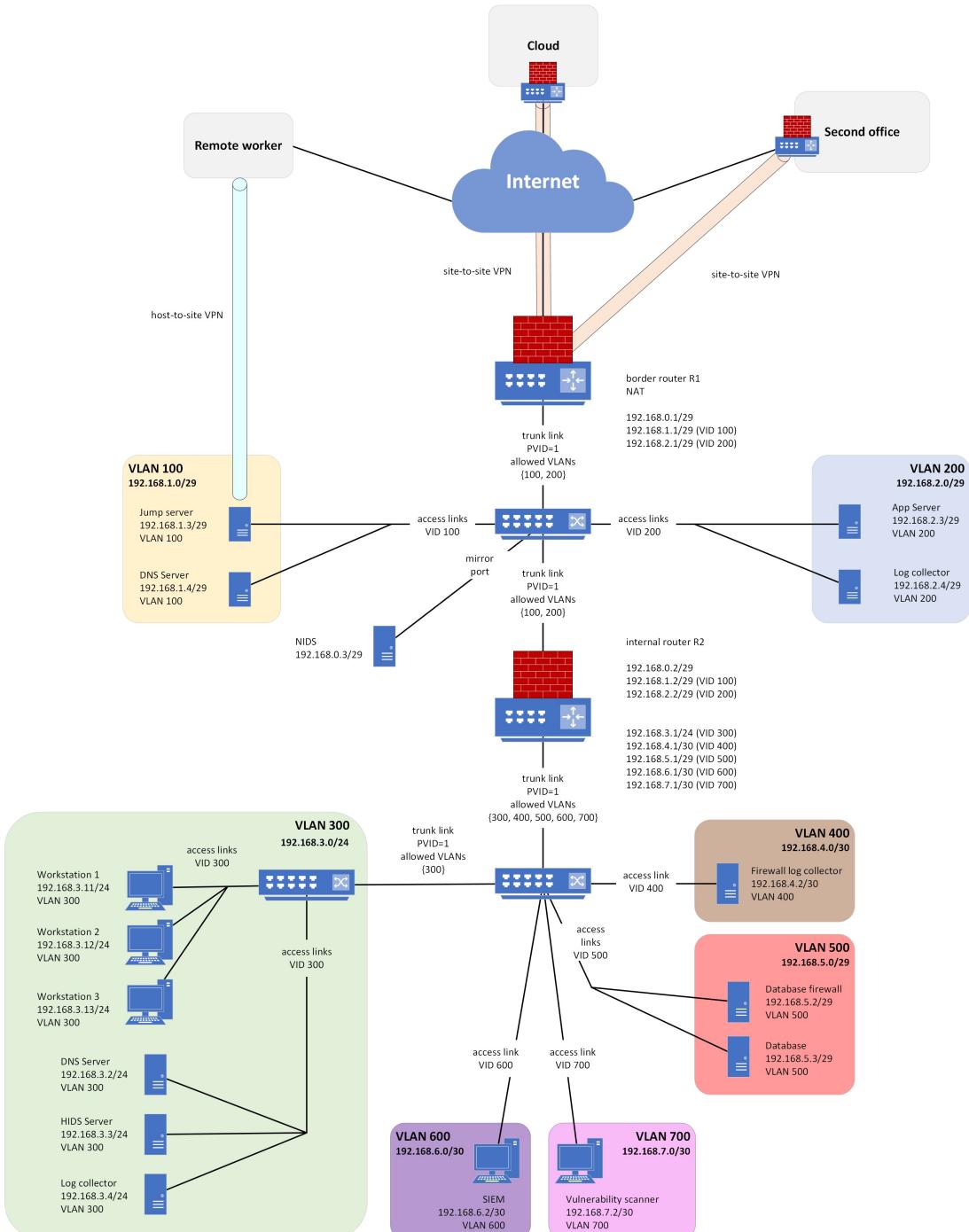


Rysunek 2: Sugerowana topologia sieci: schemat wysokopoziomowy

3. Design niskopoziomowy

W celu wstępnie zaplanowania procesu wdrażania zaprojektowanej infrastruktury, utworzyliśmy schemat niskopoziomowy sieci. Przybliża on informacje o m.in. typach połączeń między maszynami, switchami i routery, 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 topografię 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. Do realizacji SIEMA najpewniej wykorzystane zostanie rozwiązanie Wazuh, które dynamicznie przydziela porty (z ograniczonego zakresu) dla swoich agentów. Z tego powodu porty dla SIEMA zostały oznaczone jako "x".

Kolektor logów – segment niebieski	
1104/TCP	Przyjmowanie logów od serwera DNS
1203/TCP	Przyjmowanie logów od serwera aplikacyjnego
1216/TCP	Przyjmowanie logów od NIDS
1514-1515/TCP	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	
1304/TCP	Przyjmowanie logów od serwera DNS
1300/TCP	Przyjmowanie logów od serwera HIDS
1514-1515/TCP	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	
1401/TCP	Przyjmowanie logów od firewalla brzegowego (na routerze R1)
1402/TCP	Przyjmowanie logów od firewalla wewnętrznego (na routerze R2)
1405/TCP	Przyjmowanie logów od firewalla bazodanowego
1514-1515/TCP	Wysyłanie logów do SIEM'a w strefie Cyber Zone

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

NIDS	
phy-iface	Odbieranie kopii ruchu ze switcha
1216/TCP	Wysyłanie logów do kolektora w segmencie niebieskim

Tabela 4: Konfiguracja portów i usług dla NIDS

Serwer HIDS	
1305-1399/TCP	Odbieranie logów z agentów HIDS, jeden port na jednego z N agentów
1300/TCP	Wysyłanie logów do log kolektora w segmencie zielonym

Tabela 5: Konfiguracja portów i usług dla serwera HIDS

SIEM (Wazuh)	
x/TCP	Odbieranie logów od kolektora z segmentu niebieskiego
x/TCP	Odbieranie logów od kolektora z segmentu zielonego
x/TCP	Odbieranie logów od kolektora z segmentu brązowego

Tabela 6: Konfiguracja portów i usług dla SIEM

Skaner podatności	
n/a	Wszystkie porty zamknięte, zezwalanie na odpowiedzi na zainicjowane połączenia

Tabela 7: Konfiguracja portów i usług dla skanera podatności

Database firewall	
1433/TCP	Przyjmowanie zapytań SQL (reverse proxy)
1435/TCP	Przekazywanie poprawnych zapytań SQL do serwera DB (reverse proxy)
1405/TCP	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.

Serwer DNS - segment żółty	
53/TCP/UDP	Port do obsługi zapytań DNS
1104/TCP	Wysyłanie logów do log kolektora w segmencie niebieskim

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

Serwer przesiadkowy (jump server)	
13231/TCP	Port dla usługi VPN
10101/TCP	Port do komunikacji z wybranymi hostami w segmencie zielonym

Tabela 10: Konfiguracja portów i usług dla serwera przesiadkowego

Serwer aplikacyjny	
433/TCP	Port dla obsługi żądań HTTPS
1203/TCP	Wysyłanie logów do kolektora w segmencie niebieskim

Tabela 11: Konfiguracja portów i usług dla serwera aplikacyjnego

Serwer DNS - segment zielony	
53/TCP/UDP	Port do obsługi zapytań DNS
1304/TCP	Wysyłanie logów do kolektora w segmencie zielonym

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

Host biurowy (workstation)	
1-633/TCP/UDP	Porty do realizacji zadań biurowych przewidzianych dla danego stanowiska
1111/TCP	Wysyłanie logów do serwera HIDS

Tabela 13: Konfiguracja portów i usług dla hosta biurowego

Baza danych	
5432/TCP	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	Okręślone 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	Okręślone 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. Firewalli 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.

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

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.

		SOURCE							
		Internet	Border firewall (R1)	Segment ŻÓŁTY	Segment NIEBIESKI	Segment ZIELONY	Segment CZERWONY	Segment BRĄZOWY	CYBER ZONE
DESTINATION	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 Konkretnie hosty	NIE	NIE
	Segment CZERWONY	NIE	NIE	NIE	NIE	Ograniczona komunikacja Konkretnie hosty		NIE	NIE
	Segment BRĄZOWY	NIE	Przekazanie logów	NIE	NIE	NIE	Przekazanie logów z DB FW		NIE
	CYBER ZONE	Ruch skorelowany	NIE	Skan	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 wewnętrznie 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 do 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 odzwierciedlała 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 spełniają 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.

Część II

Laboratorium 2.: *Bezpieczne architektury sieci*

7. Wymagania laboratoryjne

W ramach laboratorium należało wdrożyć stworzony wcześniej projekt spełniając poniższe wymagania (z możliwością wyboru realizowanych elementów):

- Sieć
 - ◊ Uruchomienie sieci.
 - ◊ Routing & Switching.
- Segment zdalny - jedna z opcji:
 - ◊ Sieć z drugiego biura.
 - ◊ Chmura.
- Wdrożenie usług cyberbezpieczeństwa:
 - ◊ Segmentacja i segregacja sieci.
 - ◊ Firewalling VLAN.
 - ◊ Site-to-Site VPN.
 - ◊ Jedna z wybranych:
 - Pulpit zdalny dla pracownika z jump serwerem.
 - Network IDS.
 - Host IDS / EDR.
 - Skaner podatności.
 - SIEM i logi z hostów.
 - SIEM i logi firewalli.
 - SIEM i logi DNS.

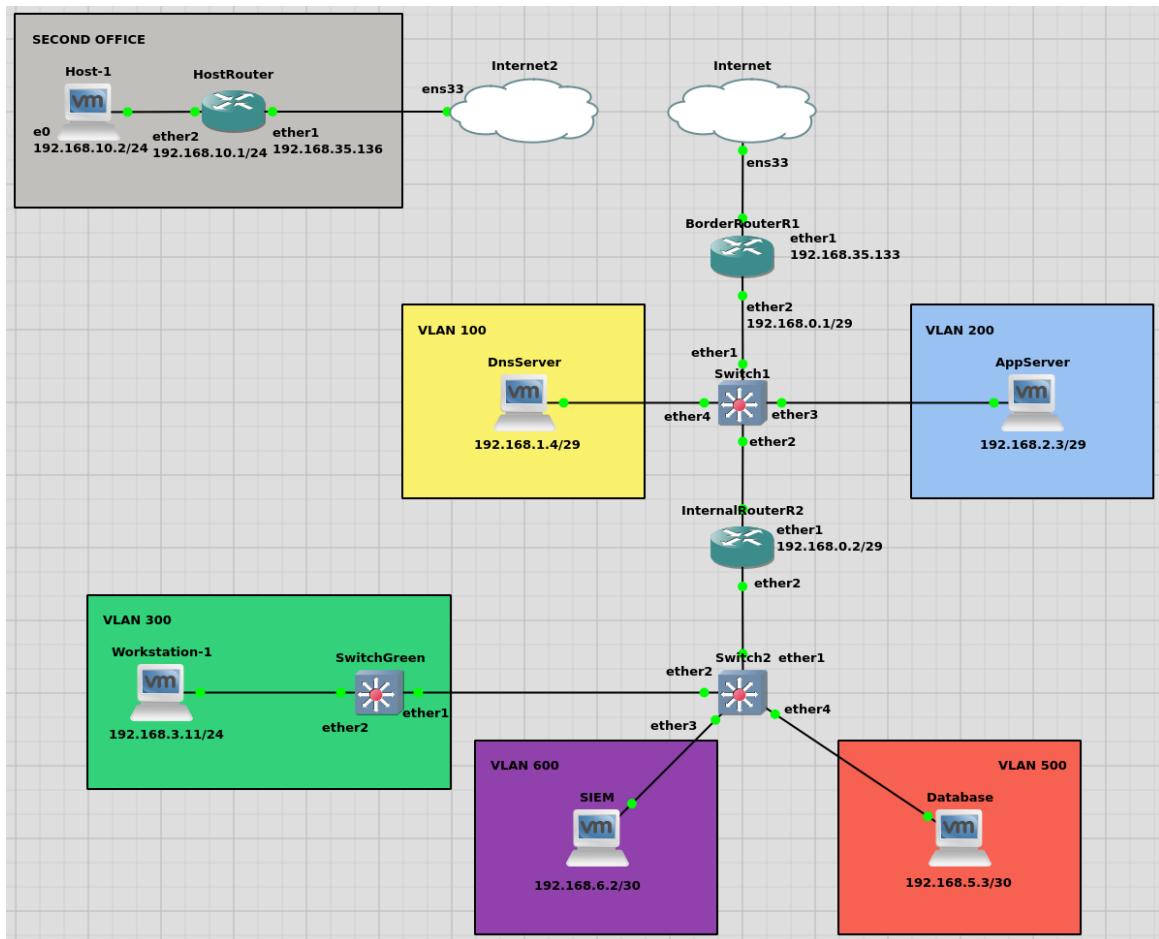
8. Wybrane przez nas elementy

Do implementacji wybraliśmy następujące elementy:

1. Główna część lokalna:
 - segment żółty (VLAN 100) – serwer DNS,
 - segment niebieski (VLAN 200) – serwer webowy,
 - segment zielony (VLAN 300) – Host workstation zainstalowanym agentem rozwiązania SIEM,
 - segment czerwony (VLAN 500) – serwer bazodanowy,
 - segment fioletowy (VLAN 600) – SIEM/Host IDS (serwer Wazuh),
2. Obszary zdalne: drugie biuro firmy.

9. Topologia sieci

Implementacja topologii sieci zawiera wybrane przez nas elementy z topologii przedstawionej w części projektowej. Całość przygotowana została w emulatorze sieci GNS3. Do emulacji hostów wykorzystane zostały maszyny wirtualne, które po odpowiednim skonfigurowaniu zostały zimportowane z VMWare Workstation do programu GNS3. Następnie zostały podpięte do infrastruktury sieciowej, w skład której wchodzą: router brzegowy, router wewnętrzny i switche w "głównym" biurze, a także router brzegowy w biurze numer 2. Wszystkie użyte urządzenia są firmy MikroTik. Wybór firmy MikroTik był dla nas istotny, ze względu na możliwość realizacji firewalla na routerze. Utworzoną topologię w GNS przedstawia rysunek 7.



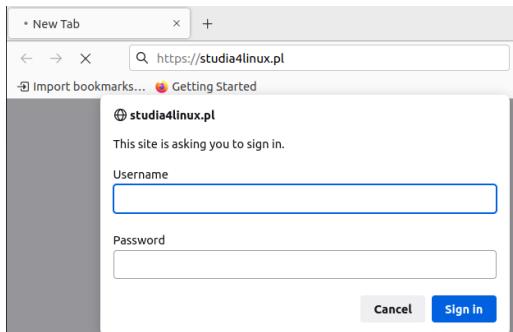
Rysunek 7: Topologia utworzonej sieci w GNS3

10. Konfiguracja komponentów sieci

10.1. Serwer aplikacyjny

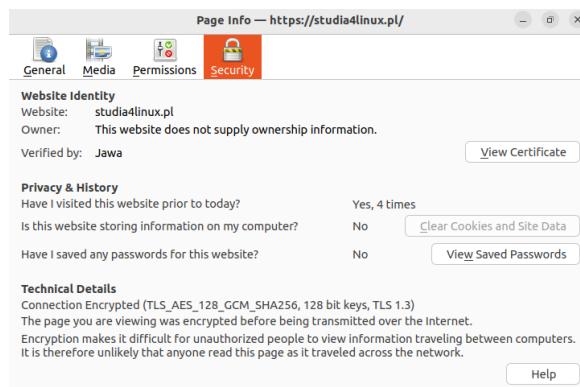
Serwer aplikacyjny, został zaimplementowany na maszynie wirtualnej z systemem Ubuntu 22.04 LTS (Jammmy Jellyfish). Maszyna w wersji Server (brak interfejsu graficznego) została pobrana ze strony <https://www.linuxvmimages.com>. Serwer aplikacyjny został zaimplementowany przy pomocy serwera apache2, a backend (renderowanie podstron) był realizowany przy pomocy modułu Flask w Python.

Pierwszym wprowadzonym elementem bezpieczeństwa był system uwierzytelniania użytkowników (przewidziany na rysunku 8), dzięki któremu osoby niepowołane nie mogą wyświetlić zawartości żadnej z podstron.



Rysunek 8: Mechanizm uwierzytelniania

Kolejnym elementem było zastosowanie komunikacji szyfrowanej protokołem TLSv1.3. 9. Otworzony został również port 80 (HTTP), jednak aplikacji nie da się używać za jego pośrednictwem – następuje automatyczne przekierowanie na protokół HTTPS.



Rysunek 9: Ustawiony certyfikat https

10.2. Serwer DNS

W strefie zdemilitaryzowanej został postawiony serwer DNS. Dzięki temu możliwe jest lokalne rozwiązywanie domeny `studia4linux.pl` na adres naszego serwera aplikacyjnego. Dodatkowo jako forwarder ustawiony został adres serwera DNS Google'a (8.8.8.8) – w przypadku braku rozwiązania domeny, lokalny serwer zapyta się o nią wskazany serwer. Dzięki temu, omawiany serwer może zostać ustawiony jako domyślny serwer DNS wszystkim hostom w sieci biurowej. Weryfikacja poprawności działania serwera DNS z poziomu stacji roboczej przedstawia rysunek 10.

```
osboxes@workstationOne:~$ nslookup studia4linux.pl
Server:      127.0.0.53
Address:      127.0.0.53#53

Non-authoritative answer:
Name:  studia4linux.pl
Address: 192.168.2.3

osboxes@workstationOne:~$ nslookup google.com
Server:      127.0.0.53
Address:      127.0.0.53#53

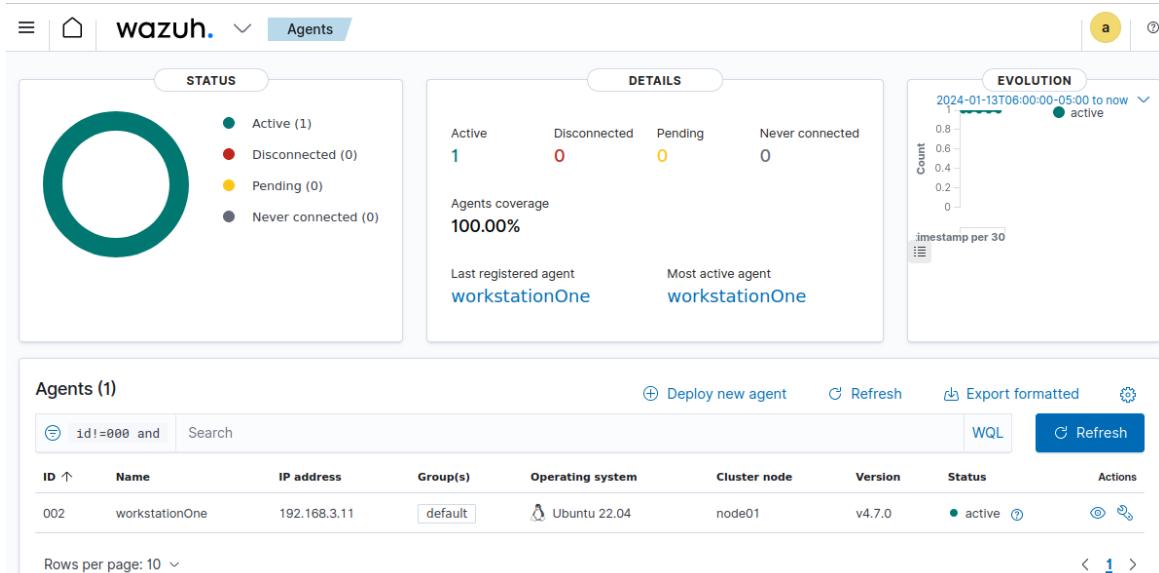
Non-authoritative answer:
Name:  google.com
Address: 142.250.75.14
Name:  google.com
Address: 2a00:1450:401b:804::200e
```

Rysunek 10: Weryfikacja poprawności działania serwera DNS z poziomu stacji roboczej: domena lokalna i publiczna

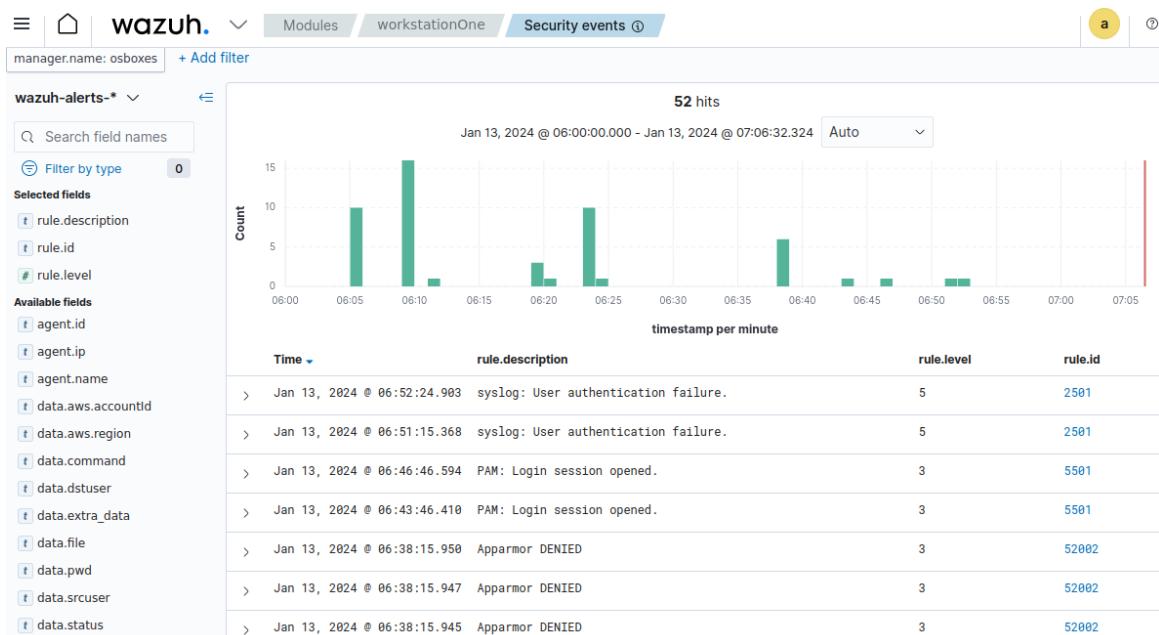
10.3. Rozwiązańe SIEM

SIEM został zaimplementowany na maszynie wirtualnej z systemem Ubuntu 22.04 LTS (Jammy Jellyfish). Maszyna w wersji Desktop została pobrana ze strony <https://osboxes.org>. Wybraliśmy rozwiązanie desktopowe ze względu na chęć zaimplementowania SIEMA z interfejsem graficznym – Wazuh.

Przyjęte rozwiązanie udostępnia end-point, do którego mogą łączyć się agenci Wazuh. Agenci następnie przesyłają do serwera Wazuh logi ze skonfigurowanych plików. Interfejs graficzny Wazuh służący do analizy zdarzeń przedstawia rysunek 12, a potwierdzający podłączenie się agenta (z hostem Workstation) rysunek 11.



Rysunek 11: Przyłączenie agenta – Host Workstation



Rysunek 12: Webowy interfejs graficzny – Wazuh

10.4. Segmentacja sieci

Sieć została podzielona na segmenty zgodnie z założeniami przedstawionymi w dokumentacji projektowej. Cały ruch pomiędzy VLANami jest routowany i filtrowany przez router wewnętrzny. Dzięki temu w przypadku awarii routera brzegowego, sieć biurowa pozostaje w pełni funkcjonalna (z pominięciem dostępu do Internetu). W celu zrealizowania podziałów na segmenty w L2, routery zostały skonfigurowane następująco:

- Konfiguracja routera brzegowego - główne biuro, rysunek 13.

```
/interface vlan
add interface=ether2 name=VLAN100 vlan-id=100
add interface=ether2 name=VLAN200 vlan-id=200
...
/ip address
add address=192.168.0.1/29 interface=ether2 network=192.168.0.0
add address=192.168.1.1/29 interface=VLAN100 network=192.168.1.0
add address=192.168.2.1/29 interface=VLAN200 network=192.168.2.0
add address=192.255.255.1/30 interface=VPN-S2S network=192.255.255.0
```

Rysunek 13: Konfiguracja vlan, router brzegowy

- Konfiguracja routera wewnętrznego - główne biuro, rysunek 14.

```
/interface vlan
add interface=ether1 name=VLAN100 vlan-id=100
add interface=ether1 name=VLAN200 vlan-id=200
add interface=ether2 name=VLAN300 vlan-id=300
add interface=ether2 name=VLAN400 vlan-id=400
add interface=ether2 name=VLAN500 vlan-id=500
add interface=ether2 name=VLAN600 vlan-id=600
add interface=ether2 name=VLAN700 vlan-id=700
...
/ip address
add address=192.168.0.2/29 interface=ether1 network=192.168.0.0
add address=192.168.3.1/24 interface=VLAN300 network=192.168.3.0
add address=192.168.4.1/29 interface=VLAN400 network=192.168.4.0
add address=192.168.5.1/29 interface=VLAN500 network=192.168.5.0
add address=192.168.6.1/30 interface=VLAN600 network=192.168.6.0
add address=192.168.7.1/30 interface=VLAN700 network=192.168.7.0
add address=192.168.1.2/29 interface=VLAN100 network=192.168.1.0
add address=192.168.2.2/29 interface=VLAN200 network=192.168.2.0
```

Rysunek 14: Konfiguracja vlan, router wewnętrzny

Pełna konfiguracja routerów została przedstawiona w sekcji 16.1. w załączniku w części IV.

Łącza pomiędzy routery zostały skonfigurowane jako łącza trunk. Pozostałe łącza (między switchami i między switchami a hostami) zostały skonfigurowane jako łącza dostępowe, na których zachodzi tagowanie ramek (VLAN ID zgodne z tymi przedstawionymi na rysunku 7). Pełna konfiguracja switchy została przedstawiona w sekcji 16.2. w załączniku w części IV.

10.5. Firewallle

Network firewallle zostały skonfigurowane na routera MikroTik dostępnych w GNS3. Konfigurację firewalla z biura nr. 2 przedstawia rysunek 15. Kontroluje on cały ruch przychodzący i wychodzący z drugiego biura.

```
/ip firewall filter
add action=accept chain=input dst-port=13231 protocol=udp src-address=\
192.168.35.133
add action=accept chain=forward dst-address=192.168.10.0/29 src-address=\
192.168.0.0/21
add action=accept chain=forward dst-address=192.168.0.0/21 src-address=\
192.168.10.0/29
/ip firewall nat
add action=masquerade chain=srcnat ipsec-policy=out,none out-interface=ether1
/ip route
add dst-address=192.168.0.0/21 gateway=VPN-S2S
```

Rysunek 15: Konfiguracja reguł firewalla - biuro nr 2

Konfiguracja firewalla brzegowego z głównego biura przedstawiona jest na rysunku 16. Kontroluje on dostęp pomiędzy biurem a siecią zewnętrzną.

```

/ip firewall filter
add action=accept chain=input comment="Site-to-Site VPN" dst-port=13231 \
    protocol=udp src-address=192.168.35.136
add action=accept chain=forward comment="Site-to-Site VPN" dst-address=\
    192.168.0.0/21 src-address=192.168.10.0/29
add action=accept chain=forward comment="Site-to-Site VPN" dst-address=\
    192.168.10.0/29 src-address=192.168.0.0/21
add action=accept chain=forward comment="HTTPS server traffic" dst-address=\
    192.168.2.3 dst-port=443,80 protocol=tcp
add action=accept chain=forward comment="Traffic to Internet" out-interface=\
    ether1 src-address=192.168.0.0/16
add action=accept chain=forward comment="Related traffic" connection-state=\
    established,related
add action=drop chain=forward comment="Drop everything"
/ip firewall nat
add action=masquerade chain=srcnat ipsec-policy=out,none out-interface=ether1
add action=dst-nat chain=dstnat comment="Redirect traffic to www server" \
    dst-port=80 in-interface=ether1 protocol=tcp to-addresses=192.168.2.3 \
    to-ports=80
add action=dst-nat chain=dstnat comment="Redirect traffic to www server" \
    dst-port=443 in-interface=ether1 protocol=tcp to-addresses=192.168.2.3 \
    to-ports=443

```

Rysunek 16: Konfiguracja reguł firewalla - router brzegowy, główne biuro

Konfiguracja firewalla wewnętrznego w głównym biurze przedstawiona jest na rysunku 17. Kontroluje on dostęp pomiędzy komponentami w sieci wewnętrznej.

```

0   ;;; DNS query
    chain=forward action=accept protocol=udp dst-address=192.168.1.4
    in-interface-list=DNS-vlans dst-port=53

1   ;;; DNS query tcp
    chain=forward action=accept protocol=tcp dst-address=192.168.1.4
    in-interface-list=DNS-vlans dst-port=53

2   ;;; DNS response
    chain=forward action=accept protocol=udp src-address=192.168.1.4
    out-interface-list=DNS-vlans dst-port=53

3   ;;; DNS response tcp
    chain=forward action=accept protocol=tcp src-address=192.168.1.4
    out-interface-list=DNS-vlans dst-port=53

4   ;;; Server WWW from VLAN 300 port 80
    chain=forward action=accept protocol=tcp dst-address=192.168.2.3
    in-interface=VLAN300 port=80

5   ;;; Server WWW response to VLAN 300 port 80
    chain=forward action=accept protocol=tcp src-address=192.168.2.3
    out-interface=VLAN300 port=80

6   ;;; Server WWW from VLAN 300 port 443
    chain=forward action=accept protocol=tcp dst-address=192.168.2.3
    in-interface=VLAN300 port=443

7   ;;; Server WWW response to VLAN 300 port 443
    chain=forward action=accept protocol=tcp src-address=192.168.2.3
    out-interface=VLAN300 port=443

8   ;;; Database access from one host
    chain=forward action=accept protocol=tcp src-address=192.168.3.11
    dst-address=192.168.5.3 port=5432

9   ;;; Database access from one host - response
    chain=forward action=accept protocol=tcp src-address=192.168.5.3
    dst-address=192.168.3.11 port=5432

10  ;;; SIEM to agents
    chain=forward action=accept protocol=tcp src-address=192.168.6.2
    dst-address-list=Wazuh-agents

11  ;;; Agents to SIEM port 1514
    chain=forward action=accept protocol=tcp dst-address=192.168.6.2
    src-address-list=Wazuh-agents port=1514

12  ;;; Agents to SIEM port 1515
    chain=forward action=accept protocol=tcp dst-address=192.168.6.2
    src-address-list=Wazuh-agents port=1515

13  ;;; Traffic to Internet
    chain=forward action=accept out-interface=ether1
    in-interface-list=Internet-vlans

14  ;;; Related traffic
    chain=forward action=accept connection-state=established,related

15  ;;; Drop everything
    chain=forward action=drop

```

Rysunek 17: Konfiguracja reguł firewalla - router wewnętrzny, główne biuro

10.6. VPN site-to-site

Jednym z wymagań laboratoryjnych było połączenie biura głównego z biurem drugim przy pomocy site-to-site VPN. W tym celu użyliśmy zaproponowanego przez Prowadzącego rozwiązania **WireGuard**. Połączenie zostało skonfigurowane pomiędzy routerem brzegowym głównego biura (rysunek 18), a routerem brzegowym drugiego biura (rysunek 19).

```
/interface wireguard
add listen-port=13231 mtu=1420 name=VPN-S2S

/interface wireguard peers
add allowed-address=192.168.10.0/29 endpoint-address=192.168.35.136 \
    endpoint-port=13231 interface=VPN-S2S public-key=\
    "kY7tyZPNhDKl9fyszNrQtoRzVSE7CwwIV5rgdW6fcg8="
```

Rysunek 18: Konfiguracja vpn site-to-site, router brzegowy głównego biura

```
/interface wireguard
add listen-port=13231 mtu=1420 name=VPN-S2S

/interface wireguard peers
add allowed-address=192.168.0.0/21 endpoint-address=192.168.35.133 \
    endpoint-port=13231 interface=VPN-S2S public-key=\
    "eauTLQzhI58HwJ6BBqRDdjYsMureXfcuCliLQ690lGI="
/ip address
add address=192.168.10.1/29 interface=ether2 network=192.168.10.0
add address=192.255.255.2/30 interface=VPN-S2S network=192.255.255.0
```

Rysunek 19: Konfiguracja vpn site-to-site, router brzegowy drugiego biura

11. Wnioski i podsumowanie

Dzięki poprzednim doświadczeniom realizacja zadania przebiegła płynniej i łatwiej niż w przypadku pierwszej styczności z GNS przy laboratorium 1. Zastosowane elementy bezpieczeństwa stanowią podstawowe środki mające na celu:

- ograniczenie możliwości ”lateral movement” w sytuacji przejęcia kontroli nad wybranym hostem przez atakującego (co zostanie udowodnione w laboratorium nr. 3),
- monitorowanie zdarzeń zachodzących na hostach czy uniemożliwienie podsłuchiwanie komunikacji zachodzącej między hostami w sieci.

Kluczowym elementem był wcześniejszy plan projektowy – punkt wyjścia do implementacji. Dzięki temu, że wykonaliśmy ten etap solidnie (wraz z adresacją, planem VLAN, macierzami komunikacji) implementacja była ”formalnością”.

W ramach realizacji projektu wykorzystaliśmy następujące narzędzia:

- Overleaf i Latex – do utworzenia niniejszego sprawozdania.
- GNS3 – do implementacji architektury sieci.
- VMWare Workstation 17 Player – jako środowisko wirtualizacyjne.

Część III

Projekt i Laboratorium 3.: *Audyt bezpieczeństwa sieci*

12. Wstęp

Celem projektu i laboratorium nr 3 było wykonanie audytu i testów bezpieczeństwa infrastruktury utworzonej w ramach poprzednich części projektu.

13. Część aktywna

13.1. Testy penetracyjne aplikacji webowej

W ramach audytu bezpieczeństwa przeprowadziliśmy dogłębne testy penetracyjne aplikacji webowej. Ponieważ jest to usługa wystawiana do sieci publicznej, jej zabezpieczenie jest kluczowe. Atakujący mogą ją wykorzystać jako początkowy punkt wejścia do sieci, z którego spróbują przeniknąć wглб infrastruktury. Oprócz testów manualnych zgodnych z metodologią OWASP WSTG, przeprowadziliśmy szereg zautomatyzowanych skanów, wykorzystując narzędzia takie jak:

- Burp Suite Active Scanner,
- Nessus Vulnerability Scanner,
- Nikto web server scanner,
- nmap – wykorzystaliśmy skrypty do enumeracji serwerów HTTP,
- DirBuster.

Podczas testów nie udało nam się zidentyfikować żadnej kwestii o wysokim poziomie ryzyka, ani potencjalnych wektorów, które w znacznym stopniu mogłyby wpłynąć na poufność, integralność lub dostępność testowanej aplikacji. Dodatkowo nie udało nam się wniknąć wглб infrastruktury wykorzystując serwer aplikacyjny jako początkowy punkt wejścia. Na rysunku 20. przedstawiamy listę wszystkich zidentyfikowanych kwestii wraz z określonym poziomem ryzyka (w raporcie Nessus widoczna jest również podatność Buffer overflow, która została potwierdzona jako false-positive podczas testów manualnych):

ID	Nazwa kwestii	Ryzyko	CVSS 3.0	Opis	Rekomendacja
studia4_001	Brak mechanizmu blokującego uwierzytelnianie	Średnie	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Aplikacja nie posiadała mechanizmów blokujących uwierzytelnianie po dokonaniu zbyt dużej liczby niepoprawnych prób uwierzytelniania. Wynikiem tego aplikacja była podatna na ataki typu brute-force na konta użytkowników.	Wprowadzenie mechanizmów blokujących zapytania wysypane z danego adresu IP lub konta użytkownika po wykonaniu zbyt wielu błędnych prób uwierzytelniania.
studia4_002	Ujawnianie informacji w nagłówkach odpowiedzi	Info	N/A	Aplikacja ujawniała nadmiarowe informacje na temat wersji wykorzystawanego serwera HTTP w nagłówkach 'server' odpowiedzi otrzymywanych od serwera. Zdradzanie takich informacji może być wykorzystane przez potencjalnych atakujących podczas enumeracji aplikacji i szukania podatności.	Wyłączenie dodawania nagłówka informującego o wykorzystywanej wersji w wysyłanych przez serwer odpowiedziach.
studia4_003	Obsługiwane nadmiarowe metody HTTP	Info	N/A	Aplikacja obsługiwała nadmiarowe metody HTTP 'HEAD' oraz 'OPTIONS'. Metody te nie są wykorzystywane przez aplikację podczas realizacji standardowych funkcjonalności. Jednocześnie mogą być one wykorzystane przez atakujących znacznie przyśpieszając działanie zautomatyzowanych narzędzi enumerujących zasoby serwera.	Zablokowanie obsługi metod HTTP 'HEAD' oraz 'OPTIONS' przez serwer.

Rysunek 20: Serwer webowy – lista wszystkich zidentyfikowanych kwestii wraz z określonym poziomem ryzyka

13.2. Testy penetracyjne infrastruktury sieciowej

Przeprowadziliśmy również testy penetracyjne infrastruktury sieciowej z poziomu sieci publicznej. W ramach testów wykryliśmy niebezpieczną konfigurację routera brzegowego:

- wiele domyślnie otwartych usług (w tym remote access) – przedstawia je rysunek 21.

```
(witat@kali)-[~]
$ sudo nmap -sS --top-ports 3000 192.168.35.133
[sudo] password for witat:
Sorry, try again.
[sudo] password for witat:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-20 14:19 CET
Nmap scan report for 192.168.35.133
Host is up (0.10s latency).
Not shown: 2993 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 61.87 seconds
```

Rysunek 21: Router brzegowy: wiele domyślnie otwartych usług, skan z sieci publicznej

- brak domyślnego **deny** na firewallu dla ruchu przychodzącego, co umożliwiło dostęp do routera z sieci zewnętrznej – wykorzystanie do tego celu usług **ssh** i **ftp** przedstawia rysunek 22a. i 22b.

(a) Wykorzystanie usługi **ssh**

```
(witat@kali)-[~]
$ ssh admin@192.168.35.133
admin@192.168.35.133's password:

KRYCY

      MMMM      MMMM      KKK      TTTTTTTTTT      KKK
      MMMMM      MMMM      KKK      TTTTTTTTTT      KKK
      MMMM      MMMM      III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
      MMMM      MMMM      III  KKKK  KKK  RRRR  000  000  TTT  III  KKKKKK
      MMMM      MMMM      III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
      MMMM      MMMM      III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 7.11.2 (c) 1999-2023      https://www.mikrotik.com/
Press F1 for help

[admin@MikroTik] > 
```

(b) Wykorzystanie usługi **ftp**

```
> ftp 192.168.35.133
Connected to 192.168.35.133.
220 MikroTik FTP server (MikroTik 7.11.2) ready
500 'OPTS': command not understood
User (192.168.35.133:(none)): admin
331 Password required for admin
Password:
230 User admin logged in
ftp> ls -a
200 PORT command successful
150 Opening data connection
skins
..
pub
226 Transfer complete
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> |
```

Rysunek 22: Uzyskanie zdalnego dostępu do routera brzegowego

Pozostawienie domyślnej konfiguracji routera (tu: faktycznie zablokowanie jedynie ruchu forwardowanego) obrazuje popularny przypadek błędów lub niedopatrzeń konfiguracyjnych często pojawiających się w projektowanych sieciach i systemach:

- pozostawienie otwartych, nieużywanych usług z domyślnymi parami loginów i haseł.
- niedodanie reguły blokującej zapytania wchodzące do routera.

Taka konfiguracja jest niedopuszczalna w środowisku produkcyjnym i powinna zostać wykryta na etapie testów przedwdrożeniowych. Dostęp do firewalla z uprawnieniami administratora z wykorzystaniem domyślnych danych logowania umożliwia Atakującemu na wprowadzenie dowolnych zmian w konfiguracji – w szczególności usunięcie niektórych reguł, które mogłyby uniemożliwić Atakującemu rozprzestrzenienie się w sieci. To pokazuje jak ważne jest przeprowadzanie audytów bezpieczeństwa w celu identyfikacji i mitygacji takich zagrożeń wynikających najczęściej z ludzkich niedopatrzeń. Mimo swej prostoty, tego rodzaju błędy nie są czymś niespotykanym w realnych środowiskach produkcyjnych.

Dalsze kroki eksplotacji znalezionych luk bezpieczeństwa nie były kontynuowane, ponieważ wymagałyby modyfikacji reguł firewalla w działającej sieci produkcyjnej. To mogłoby negatywnie wpłynąć na dostępność i poufność procesów zachodzących wewnątrz niej.

Rekomendacja – dodać następujące reguły do firewalli:

```
add action=drop chain=input comment="Drop unmatched"
add action=drop chain=output comment="Drop unmatched"
```

14. Audyt względem standardu

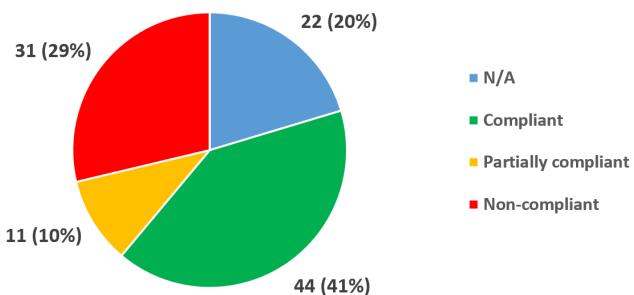
Po przeprowadzeniu technik ofensywnych przeszliśmy do oceny bezpieczeństwa wzgędem kontroli pochodzących z NIST Cybersecurity Framework. Wyjściowym dokumentem była checklista <https://www.nist.gov/document/2018-04-16frameworkv11core1x1sx>, która w formie wypełnionej została udostępniona w sekcji 17. w załączniku w części IV. Kolumna "Ocena" arkusza zawiera ocenę dla każdej kontroli przyjmując jedną z czterech wartości:

- 1 – zaprojektowany system spełnia daną kontrolę,
- 0,5 – zaprojektowany system częściowo spełnia daną kontrolę, uzasadnienie znajduje się w kolumnie o etykiecie "Komentarz".
- 0 – zaprojektowany system nie spełnia danej kontroli,
- N/A – *Not-applicable*, dana kontrola nie ma zastosowania przy zaprojektowanym systemie.

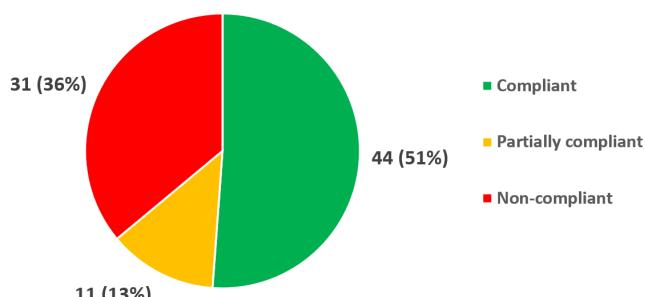
W wyniku sprawdzenia zgodności systemu ze standardem, uzyskaliśmy następujące wyniki:

- 22 nieaplikowalne kontrole,
- 44 spełnione kontrole,
- 11 częściowo spełnionych kontroli,
- 31 niespełnionych kontroli – wynikające głównie z braku definicji procesów i procedur bezpieczeństwa.

Zwizualizowaliśmy uzyskane wyniki na diagramach kołowych. Wyniki z uwzględnieniem nieaplikowalnych kontroli przedstawia rysunek 23, a bez uwzględnienia nieaplikowalnych kontroli rysunek 24.



Rysunek 23: Wyniki z uwzględnieniem nieaplikowalnych kontroli



Rysunek 24: Wyniki bez uwzględnienia nieaplikowalnych kontroli

15. Podsumowanie

Projekt pokazał nam istotę przeprowadzania regularnych audytów oraz testów bezpieczeństwa. Ich wykonanie pomaga zweryfikować poprawność implementacji i konfiguracji tworzonej infrastruktury z uwzględnieniem zgodności z wyjściowymi założeniami. Sam framework NIST na pierwszy rzut oka wydawał się długim dokumentem, jednak wraz z kolejnymi punktami checklisty dyskusja w zespole ożywała, a proces audytu przebiegł sprawnie i ciekawie.

Cieszymy się, że projekty oraz laboratoria tworzą jedną całość i podsumowują tematy omówione na wykłada- dach (nie tylko BEKOMu, ale i innych przedmiotów). Tym sposobem przedmiot jest kompletny, wartościowy i pozytywnie wyróżnia się na tle szerokiej oferty edukacyjnej naszego wydziału.

Część IV

Załączniki

16. Konfiguracja komponentów sieciowych (laboratorium 2)

16.1. Routery

16.1.1. Konfiguracja routera brzegowego

```
1 # 2024-01-13 12:39:32 by RouterOS 7.11.2
2 # software id =
3 #
4 /interface ethernet
5 set [ find default-name=ether1 ] disable-running-check=no
6 set [ find default-name=ether2 ] disable-running-check=no
7 set [ find default-name=ether3 ] disable-running-check=no
8 set [ find default-name=ether4 ] disable-running-check=no
9 set [ find default-name=ether5 ] disable-running-check=no
10 set [ find default-name=ether6 ] disable-running-check=no
11 set [ find default-name=ether7 ] disable-running-check=no
12 set [ find default-name=ether8 ] disable-running-check=no
13 /interface wireguard
14 add listen-port=13231 mtu=1420 name=VPN-S2S
15 /interface vlan
16 add interface=ether2 name=VLAN100 vlan-id=100
17 add interface=ether2 name=VLAN200 vlan-id=200
18 /disk
19 set slot1 slot=slot1 type=hardware
20 set slot2 slot=slot2 type=hardware
21 set slot3 slot=slot3 type=hardware
22 set slot4 slot=slot4 type=hardware
23 set slot5 slot=slot5 type=hardware
24 /interface wireless security-profiles
25 set [ find default=yes ] supplicant-identity=MikroTik
26 /port
27 set 0 name=serial0
28 /interface wireguard peers
29 add allowed-address=192.168.10.0/29 endpoint-address=192.168.35.136 \
30     endpoint-port=13231 interface=VPN-S2S public-key=\
31     "kY7tyZPNhDK19fyszNrQtoRzVSE7CwwIV5rgdW6fcg8="
32 /ip address
33 add address=192.168.0.1/29 interface=ether2 network=192.168.0.0
34 add address=192.168.1.1/29 interface=VLAN100 network=192.168.1.0
35 add address=192.168.2.1/29 interface=VLAN200 network=192.168.2.0
36 add address=192.255.255.1/30 interface=VPN-S2S network=192.255.255.0
37 /ip dhcp-client
38 add interface=ether1
39 /ip firewall filter
40 add action=accept chain=input comment="Site-to-Site VPN" dst-port=13231 \
41     protocol=udp src-address=192.168.35.136
42 add action=accept chain=forward comment="Site-to-Site VPN" dst-address=\
43     192.168.0.21 src-address=192.168.10.0/29
44 add action=accept chain=forward comment="Site-to-Site VPN" dst-address=\
45     192.168.10.0/29 src-address=192.168.0.0/21
46 add action=accept chain=forward comment="HTTPS server traffic" dst-address=\
47     192.168.2.3 dst-port=443,80 protocol=tcp
48 add action=accept chain=forward comment="Traffic to Internet" out-interface=\
49     ether1 src-address=192.168.0.0/16
50 add action=accept chain=forward comment="Related traffic" connection-state=\
51     established,related
52 add action=drop chain=forward comment="Drop everything"
53 /ip firewall nat
54 add action=masquerade chain=srcnat ipsec-policy=out,none out-interface=ether1
```

```

55 add action=dst-nat chain=dstnat comment="Redirect traffic to www server" \
56     dst-port=80 in-interface=ether1 protocol=tcp to-addresses=192.168.2.3 \
57     to-ports=80
58 add action=dst-nat chain=dstnat comment="Redirect traffic to www server" \
59     dst-port=443 in-interface=ether1 protocol=tcp to-addresses=192.168.2.3 \
60     to-ports=443
61 /ip route
62 add dst-address=192.168.3.0/24 gateway=192.168.0.2
63 add dst-address=192.168.4.0/29 gateway=192.168.0.2
64 add dst-address=192.168.5.0/29 gateway=192.168.0.2
65 add dst-address=192.168.6.0/30 gateway=192.168.0.2
66 add dst-address=192.168.7.0/30 gateway=192.168.0.2
67 add dst-address=192.168.10.0/29 gateway=VPN-S2S
68 /system note
69 set show-at-login=no

```

16.1.2. Konfiguracja routera wewnętrznego

```

1 # 2024-01-13 12:40:13 by RouterOS 7.11.2
2 # software id =
3 #
4 /interface ethernet
5 set [ find default-name=ether1 ] disable-running-check=no
6 set [ find default-name=ether2 ] disable-running-check=no
7 set [ find default-name=ether3 ] disable-running-check=no
8 set [ find default-name=ether4 ] disable-running-check=no
9 set [ find default-name=ether5 ] disable-running-check=no
10 set [ find default-name=ether6 ] disable-running-check=no
11 set [ find default-name=ether7 ] disable-running-check=no
12 set [ find default-name=ether8 ] disable-running-check=no
13 /interface vlan
14 add interface=ether1 name=VLAN100 vlan-id=100
15 add interface=ether1 name=VLAN200 vlan-id=200
16 add interface=ether2 name=VLAN300 vlan-id=300
17 add interface=ether2 name=VLAN400 vlan-id=400
18 add interface=ether2 name=VLAN500 vlan-id=500
19 add interface=ether2 name=VLAN600 vlan-id=600
20 add interface=ether2 name=VLAN700 vlan-id=700
21 /disk
22 set slot1 slot=slot1 type=hardware
23 set slot2 slot=slot2 type=hardware
24 set slot3 slot=slot3 type=hardware
25 set slot4 slot=slot4 type=hardware
26 set slot5 slot=slot5 type=hardware
27 set slot6 slot=slot6 type=hardware
28 /interface list
29 add name=Internet-vlans
30 add name=DNS-vlans
31 /interface wireless security-profiles
32 set [ find default=yes ] supplicant-identity=MikroTik
33 /port
34 set 0 name=serial0
35 /interface list member
36 add interface=VLAN300 list=Internet-vlans
37 add interface=VLAN600 list=Internet-vlans
38 add interface=VLAN100 list=Internet-vlans
39 add interface=VLAN200 list=Internet-vlans
40 add interface=VLAN200 list=DNS-vlans
41 add interface=VLAN300 list=DNS-vlans
42 add interface=VLAN600 list=DNS-vlans
43 /ip address
44 add address=192.168.0.2/29 interface=ether1 network=192.168.0.0
45 add address=192.168.3.1/24 interface=VLAN300 network=192.168.3.0
46 add address=192.168.4.1/29 interface=VLAN400 network=192.168.4.0
47 add address=192.168.5.1/29 interface=VLAN500 network=192.168.5.0
48 add address=192.168.6.1/30 interface=VLAN600 network=192.168.6.0
49 add address=192.168.7.1/30 interface=VLAN700 network=192.168.7.0
50 add address=192.168.1.2/29 interface=VLAN100 network=192.168.1.0
51 add address=192.168.2.2/29 interface=VLAN200 network=192.168.2.0

```

```

52 /ip firewall address-list
53 add address=192.168.3.11 list=Wazuh-agents
54 /ip firewall filter
55 add action=accept chain=forward comment="DNS query" dst-address=192.168.1.4 \
56 dst-port=53 in-interface-list=DNS-vlans protocol=udp
57 add action=accept chain=forward comment="DNS query tcp" dst-address=192.168.1.4 \
58 dst-port=53 in-interface-list=DNS-vlans protocol=tcp
59 add action=accept chain=forward comment="DNS response" dst-port=53 \
60 out-interface-list=DNS-vlans protocol=udp src-address=192.168.1.4
61 add action=accept chain=forward comment="DNS response tcp" dst-port=53 \
62 out-interface-list=DNS-vlans protocol=tcp src-address=192.168.1.4
63 add action=accept chain=forward comment="Server WWW from VLAN 300 port 80" \
64 dst-address=192.168.2.3 in-interface=VLAN300 port=80 protocol=tcp
65 add action=accept chain=forward comment=\
66 "Server WWW response to VLAN 300 port 80" out-interface=VLAN300 port=80 \
67 protocol=tcp src-address=192.168.2.3
68 add action=accept chain=forward comment="Server WWW from VLAN 300 port 443" \
69 dst-address=192.168.2.3 in-interface=VLAN300 port=443 protocol=tcp
70 add action=accept chain=forward comment=\
71 "Server WWW response to VLAN 300 port 443" out-interface=VLAN300 port=443 \
72 protocol=tcp src-address=192.168.2.3
73 add action=accept chain=forward comment="Database access from one host" \
74 dst-address=192.168.5.3 port=5432 protocol=tcp src-address=192.168.3.11
75 add action=accept chain=forward comment=\
76 "Database access from one host - response" dst-address=192.168.3.11 port=\
77 5432 protocol=tcp src-address=192.168.5.3
78 add action=accept chain=forward comment="SIEM to agents" dst-address-list=\
79 Wazuh-agents protocol=tcp src-address=192.168.6.2
80 add action=accept chain=forward comment="Agents to SIEM port 1514" dst-address=\
81 192.168.6.2 port=1514 protocol=tcp src-address-list=Wazuh-agents
82 add action=accept chain=forward comment="Agents to SIEM port 1515" dst-address=\
83 192.168.6.2 port=1515 protocol=tcp src-address-list=Wazuh-agents
84 add action=accept chain=forward comment="Traffic to Internet" \
85 in-interface-list=Internet-vlans out-interface=ether1
86 add action=accept chain=forward comment="Related traffic" connection-state=\
87 established,related
88 add action=drop chain=forward comment="Drop everything"
89 /ip route
90 add gateway=192.168.0.1
91 /system note
92 set show-at-login=no

```

16.1.3. Konfiguracja routera w drugim biurze

```

1 # 2024-01-13 12:40:37 by RouterOS 7.11.2
2 # software id =
3 #
4 /interface ethernet
5 set [ find default-name=ether1 ] disable-running-check=no
6 set [ find default-name=ether2 ] disable-running-check=no
7 set [ find default-name=ether3 ] disable-running-check=no
8 set [ find default-name=ether4 ] disable-running-check=no
9 set [ find default-name=ether5 ] disable-running-check=no
10 set [ find default-name=ether6 ] disable-running-check=no
11 set [ find default-name=ether7 ] disable-running-check=no
12 set [ find default-name=ether8 ] disable-running-check=no
13 /interface wireguard
14 add listen-port=13231 mtu=1420 name=VPN-S2S
15 /disk
16 set slot1 slot=slot1 type=hardware
17 set slot2 slot=slot2 type=hardware
18 set slot3 slot=slot3 type=hardware
19 set slot4 slot=slot4 type=hardware
20 set slot5 slot=slot5 type=hardware
21 set slot6 slot=slot6 type=hardware
22 set slot7 slot=slot7 type=hardware
23 /interface wireless security-profiles
24 set [ find default=yes ] supplicant-identity=MikroTik
25 /port

```

```

26 set 0 name=serial0
27 /interface wireguard peers
28 add allowed-address=192.168.0.0/21 endpoint-address=192.168.35.133 \
29   endpoint-port=13231 interface=VPN-S2S public-key=\
30   "eauTLQzhi58HwJ6BBqRDDjYsMureXfcuCliLQ6901GI="
31 /ip address
32 add address=192.168.10.1/29 interface=ether2 network=192.168.10.0
33 add address=192.255.255.2/30 interface=VPN-S2S network=192.255.255.0
34 /ip dhcp-client
35 add interface=ether1
36 /ip dns
37 set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4
38 /ip firewall filter
39 add action=accept chain=input dst-port=13231 protocol=udp src-address=\
40   192.168.35.133
41 add action=accept chain=forward dst-address=192.168.10.0/29 src-address=\
42   192.168.0.0/21
43 add action=accept chain=forward dst-address=192.168.0.0/21 src-address=\
44   192.168.10.0/29
45 /ip firewall nat
46 add action=masquerade chain=srcnat ipsec-policy=out,none out-interface=ether1
47 /ip route
48 add dst-address=192.168.0.0/21 gateway=VPN-S2S
49 /system note
50 set show-at-login=no

```

16.2. Switche

16.2.1. Konfiguracja switcha S1

```
1 # jan/13/2024 12:42:43 by RouterOS 7.8
2 # software id =
3 #
4 /interface bridge
5 add name=bridge protocol-mode=none vlan-filtering=yes
6 /interface ethernet
7 set [ find default-name=ether1 ] disable-running-check=no
8 set [ find default-name=ether2 ] disable-running-check=no
9 set [ find default-name=ether3 ] disable-running-check=no
10 set [ find default-name=ether4 ] disable-running-check=no
11 set [ find default-name=ether5 ] disable-running-check=no
12 set [ find default-name=ether6 ] disable-running-check=no
13 set [ find default-name=ether7 ] disable-running-check=no
14 set [ find default-name=ether8 ] disable-running-check=no
15 set [ find default-name=ether9 ] disable-running-check=no
16 set [ find default-name=ether10 ] disable-running-check=no
17 set [ find default-name=ether11 ] disable-running-check=no
18 set [ find default-name=ether12 ] disable-running-check=no
19 set [ find default-name=ether13 ] disable-running-check=no
20 set [ find default-name=ether14 ] disable-running-check=no
21 set [ find default-name=ether15 ] disable-running-check=no
22 set [ find default-name=ether16 ] disable-running-check=no
23 set [ find default-name=ether17 ] disable-running-check=no
24 set [ find default-name=ether18 ] disable-running-check=no
25 set [ find default-name=ether19 ] disable-running-check=no
26 set [ find default-name=ether20 ] disable-running-check=no
27 set [ find default-name=ether21 ] disable-running-check=no
28 set [ find default-name=ether22 ] disable-running-check=no
29 set [ find default-name=ether23 ] disable-running-check=no
30 set [ find default-name=ether24 ] disable-running-check=no
31 set [ find default-name=ether25 ] disable-running-check=no
32 set [ find default-name=ether26 ] disable-running-check=no
33 set [ find default-name=ether27 ] disable-running-check=no
34 set [ find default-name=ether28 ] disable-running-check=no
35 /disk
36 set slot1 slot=slot1
37 set slot2 slot=slot2
38 set slot3 slot=slot3
39 set slot4 slot=slot4
40 set slot5 slot=slot5
41 /interface wireless security-profiles
42 set [ find default=yes ] supplicant-identity=MikroTik
43 /port
44 set 0 name=serial0
45 /interface bridge port
46 add bridge=bridge interface=ether1
47 add bridge=bridge interface=ether2
48 add bridge=bridge interface=ether3 pvid=200
49 add bridge=bridge interface=ether4 pvid=100
50 /interface bridge vlan
51 add bridge=bridge tagged=ether1,ether2 vlan-ids=100
52 add bridge=bridge tagged=ether1,ether2 vlan-ids=200
53 /ip dhcp-client
54 # DHCP client can not run on slave or passthrough interface!
55 add interface=ether1
```

16.2.2. Konfiguracja switcha S2

```
1 # jan/13/2024 12:42:13 by RouterOS 7.8
2 # software id =
3 #
4 /interface bridge
5 add name=bridge protocol-mode=none vlan-filtering=yes
6 /interface ethernet
```

```

7 set [ find default-name=ether1 ] disable-running-check=no
8 set [ find default-name=ether2 ] disable-running-check=no
9 set [ find default-name=ether3 ] disable-running-check=no
10 set [ find default-name=ether4 ] disable-running-check=no
11 set [ find default-name=ether5 ] disable-running-check=no
12 set [ find default-name=ether6 ] disable-running-check=no
13 set [ find default-name=ether7 ] disable-running-check=no
14 set [ find default-name=ether8 ] disable-running-check=no
15 set [ find default-name=ether9 ] disable-running-check=no
16 set [ find default-name=ether10 ] disable-running-check=no
17 set [ find default-name=ether11 ] disable-running-check=no
18 set [ find default-name=ether12 ] disable-running-check=no
19 set [ find default-name=ether13 ] disable-running-check=no
20 set [ find default-name=ether14 ] disable-running-check=no
21 set [ find default-name=ether15 ] disable-running-check=no
22 set [ find default-name=ether16 ] disable-running-check=no
23 set [ find default-name=ether17 ] disable-running-check=no
24 set [ find default-name=ether18 ] disable-running-check=no
25 set [ find default-name=ether19 ] disable-running-check=no
26 set [ find default-name=ether20 ] disable-running-check=no
27 set [ find default-name=ether21 ] disable-running-check=no
28 set [ find default-name=ether22 ] disable-running-check=no
29 set [ find default-name=ether23 ] disable-running-check=no
30 set [ find default-name=ether24 ] disable-running-check=no
31 set [ find default-name=ether25 ] disable-running-check=no
32 set [ find default-name=ether26 ] disable-running-check=no
33 set [ find default-name=ether27 ] disable-running-check=no
34 set [ find default-name=ether28 ] disable-running-check=no
35 /disk
36 set slot1 slot=slot1
37 set slot2 slot=slot2
38 set slot3 slot=slot3
39 set slot4 slot=slot4
40 set slot5 slot=slot5
41 /interface wireless security-profiles
42 set [ find default=yes ] supplicant-identity=MikroTik
43 /port
44 set 0 name=serial0
45 /interface bridge port
46 add bridge=bridge interface=ether1
47 add bridge=bridge interface=ether2 pvid=300
48 add bridge=bridge interface=ether3 pvid=600
49 add bridge=bridge interface=ether4 pvid=500
50 /interface bridge vlan
51 add bridge=bridge tagged=ether1 vlan-ids=300
52 add bridge=bridge tagged=ether1 vlan-ids=400
53 add bridge=bridge tagged=ether1 vlan-ids=500
54 add bridge=bridge tagged=ether1 vlan-ids=600
55 add bridge=bridge tagged=ether1 vlan-ids=700
56 /ip dhcp-client
57 # DHCP client can not run on slave or passthrough interface!
58 add interface=ether1

```

16.2.3. Konfiguracja switcha S3 (VLAN 300)

To urządzenie jest access switchem, nie wymagało wprowadzania dodatkowej konfiguracji. Przełączka jedynie ruch wewnętrz VLANu 300, wszystkie jego łącza są łączami access. Ruch tagowany jest przez switch S2.

17. Tabela względem NIST CSF

Na dalszych stronach przedstawiona została wypełniona tabela (wyjściowy dokument: <https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx>) względem NIST CSF.

Function	Category	Subcategory	Informative References	Ocena	Komentarz
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5 	N/A	
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5 	1	
		ID.AM-3: Organizational communication and data flows are mapped	<ul style="list-style-type: none"> CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 	1	
		ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 	N/A	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 	1	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 	N/A	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	<ul style="list-style-type: none"> COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12 	N/A	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	<ul style="list-style-type: none"> COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8 	N/A	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<ul style="list-style-type: none"> COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14 	N/A	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	<ul style="list-style-type: none"> COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 	N/A	
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., disaster recovery, business continuity, and emergency preparedness)	<ul style="list-style-type: none"> COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14 	N/A	
Risk Assessment (ID.RA)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational cybersecurity policy is established and communicated	<ul style="list-style-type: none"> CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families 	0,5	W kontekście dozwolonej komunikacji między komponentami i sieciami
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	<ul style="list-style-type: none"> CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PM-11, SA-14 	N/A	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	<ul style="list-style-type: none"> CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families 	0	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	<ul style="list-style-type: none"> COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 	0	
		ID.RA-1: Asset vulnerabilities are identified and documented	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 	1	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 	1	
		ID.RA-3: Threats, both internal and external, are identified and documented	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 	1	
		ID.RA-4: Potential business impacts and likelihoods are identified	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11 	1	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 	1	
		ID.RA-6: Risk responses are identified and prioritized	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9 	1	
Risk Management Strategy (ID.RM)	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9 	0	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<ul style="list-style-type: none"> COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9 	0	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical	<ul style="list-style-type: none"> COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-11 	N/A	
		ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	<ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9 	0	
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk	<ul style="list-style-type: none"> COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 	N/A	

	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	<ul style="list-style-type: none"> assessment process ID-SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization. ID-SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. ID-SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers 	<ul style="list-style-type: none"> NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9 COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR 6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 	N/A	
		<ul style="list-style-type: none"> PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes 	<ul style="list-style-type: none"> CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 	0,5	W obrębie hostów zastosowano politykę bezpiecznych haseł
		<ul style="list-style-type: none"> PR.AC-2: Physical access to assets is managed and protected 	<ul style="list-style-type: none"> COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 	N/A	
		<ul style="list-style-type: none"> PR.AC-3: Remote access is managed 	<ul style="list-style-type: none"> CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15 	0,5	VPN site-to-site, brak wprowadzonego jump servera + słabe zabezpieczenie routera
		<ul style="list-style-type: none"> PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties 	<ul style="list-style-type: none"> CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 	1	
		<ul style="list-style-type: none"> PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) 	<ul style="list-style-type: none"> CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 	1	
		<ul style="list-style-type: none"> PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions 	<ul style="list-style-type: none"> CIS CSC 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013 A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 	0	
		<ul style="list-style-type: none"> PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) 	<ul style="list-style-type: none"> CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 	1	
		<ul style="list-style-type: none"> PR.AT-1: All users are informed and trained 	<ul style="list-style-type: none"> CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13 	1	
		<ul style="list-style-type: none"> PR.AT-2: Privileged users understand their roles and responsibilities 	<ul style="list-style-type: none"> CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 	1	
		<ul style="list-style-type: none"> PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities 	<ul style="list-style-type: none"> CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SC-16 	N/A	
		<ul style="list-style-type: none"> PR.AT-4: Senior executives understand their roles and responsibilities 	<ul style="list-style-type: none"> CIS CSC 17 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 	1	
		<ul style="list-style-type: none"> PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities 	<ul style="list-style-type: none"> CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13 	1	
		<ul style="list-style-type: none"> PR.DS-1: Data-at-rest is protected 	<ul style="list-style-type: none"> CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 	1	
		<ul style="list-style-type: none"> PR.DS-2: Data-in-transit is protected 	<ul style="list-style-type: none"> CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 	0,5	Tylko dla dostępu do aplikacji webowej z sieci zewnętrznej Internet
		<ul style="list-style-type: none"> PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition 	<ul style="list-style-type: none"> CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 	0	
		<ul style="list-style-type: none"> PR.DS-4: Adequate capacity to ensure availability is maintained 	<ul style="list-style-type: none"> CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 	0	
		<ul style="list-style-type: none"> PR.DS-5: Protections against data leaks are implemented 	<ul style="list-style-type: none"> CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 	0,5	Dostęp do danych poufnych jest możliwy jedynie z określonych stacji roboczych. W przypadku ich przejęcia, dane mogą być dalej eksfiltrowane przez Atakujących
		<ul style="list-style-type: none"> PR.DS-6: Integrity checking 	CIS CSC 2, 3		

PROTECT (PR)	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	<ul style="list-style-type: none"> COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 	0	
		PR.DS-7: The development and testing environment(s) are separate from the production environment	<ul style="list-style-type: none"> COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2 	1	możemy uruchomić drugą VM z całym GNS
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	<ul style="list-style-type: none"> COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7 	0	
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<ul style="list-style-type: none"> CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 	0,5	Systemy za wyjątkiem routerów zostały zaprojektowane zgodnie z koncepcją najmniejszej funkcjonalności (dodawanie jedynie wymaganych funkcji)
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	<ul style="list-style-type: none"> CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.3.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 	0	
		PR.IP-3: Configuration change control processes are in place	<ul style="list-style-type: none"> CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 	0	
		PR.IP-4: Backups of information are conducted, maintained, and tested	<ul style="list-style-type: none"> CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 	0	
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	<ul style="list-style-type: none"> COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 	N/A	
		PR.IP-6: Data is destroyed according to policy	<ul style="list-style-type: none"> COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 	0	
		PR.IP-7: Protection processes are improved	<ul style="list-style-type: none"> COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 	1	
		PR.IP-8: Effectiveness of protection technologies is shared	<ul style="list-style-type: none"> COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 	1	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	<ul style="list-style-type: none"> CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 	0,5	Mamy backupy używanych maszyn wirtualnych. W przypadku incydentu, zaatakowaną maszyną można odpiąć od sieci i zbadać, a na
		PR.IP-10: Response and recovery plans are tested	<ul style="list-style-type: none"> CIS CSC 19, 20 COBIT 5 DS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14 	0	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<ul style="list-style-type: none"> CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 	1	
		PR.IP-12: A vulnerability management plan is developed and implemented	<ul style="list-style-type: none"> CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 	0	
		PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	<ul style="list-style-type: none"> COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6 	0,5	Wazuh + część audytowa była realizowana w obecności całego zespołu cybersecurity, który zarejestrował wszystkie
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<ul style="list-style-type: none"> CIS CSC 3, 5 COBIT 5 DS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4 	1	
		PR.PT-1: Audit log records are determined, documented, implemented, and reviewed in accordance with policy	<ul style="list-style-type: none"> CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO1.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family 	1	
		PR.PT-2: Removable media is protected and its use restricted according to policy	<ul style="list-style-type: none"> CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 	0	
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	<ul style="list-style-type: none"> CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7 	1	
		PR.PT-4: Communications and control networks are protected	<ul style="list-style-type: none"> CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 	0,5	Brak szyfrowanych połączeń w sieci lokalnej. Pozostała kontrola na firewallach
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<ul style="list-style-type: none"> COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 	0	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	DE.AE-1: A baseline of network operations and expected data flows for new and existing assets is established and	<ul style="list-style-type: none"> CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 	0,5	Bez kontroli data flows (np. https://www.mape.pl)

		USES AND SYSTEMS IS ESTABLISHED AND MANAGED	PICTURE	PICTURE
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	<ul style="list-style-type: none"> ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 		
		<ul style="list-style-type: none"> CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 	1	
		<ul style="list-style-type: none"> CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 	0,5	Tyko Workstation(s)
		<ul style="list-style-type: none"> CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.12.4.1, A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4 	1	
		<ul style="list-style-type: none"> CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 	1	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<ul style="list-style-type: none"> CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-7, SI-4 	0	
		<ul style="list-style-type: none"> COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 	0	
		<ul style="list-style-type: none"> CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 	1	
		<ul style="list-style-type: none"> CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8 	0	
		<ul style="list-style-type: none"> CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44 	0	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	<ul style="list-style-type: none"> COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 	N/A	
		<ul style="list-style-type: none"> CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 	0	
		<ul style="list-style-type: none"> CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5 	1	
		<ul style="list-style-type: none"> CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 	0	
		<ul style="list-style-type: none"> COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SI-4, PM-14 	0	
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	<ul style="list-style-type: none"> DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability 	0	
		<ul style="list-style-type: none"> DE.DP-2: Detection activities comply with all applicable requirements 	0	
		<ul style="list-style-type: none"> DE.DP-3: Detection processes are tested 	1	
		<ul style="list-style-type: none"> DE.DP-4: Event detection information is communicated 	1	
		<ul style="list-style-type: none"> DE.DP-5: Detection processes are continuously improved 	1	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	<ul style="list-style-type: none"> RS.RP-1: Response plan is executed during or after an incident 	0	
		<ul style="list-style-type: none"> RS.CO-1: Personnel know their roles and order of operations when a response is needed 	0	
		<ul style="list-style-type: none"> RS.CO-2: Incidents are reported consistent with established criteria 	1	
		<ul style="list-style-type: none"> RS.CO-3: Information is shared consistent with response plans 	0	
		<ul style="list-style-type: none"> RS.CO-4: Coordination with stakeholders occurs consistent with response plans 	N/A	
		<ul style="list-style-type: none"> RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness 	N/A	
		<ul style="list-style-type: none"> RS.CO-6: Notifications from detection systems are investigated 	1	
		<ul style="list-style-type: none"> COBIT 5 DSS02.02 		

RESPONSE (RS)	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	<p>RS.AN-2: The impact of the incident is understood</p> <ul style="list-style-type: none"> ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4 	1	
		<p>RS.AN-3: Forensics are performed</p> <ul style="list-style-type: none"> COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4 	1	
		<p>RS.AN-4: Incidents are categorized consistent with response plans</p> <ul style="list-style-type: none"> CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 	0	
		<p>RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the</p> <ul style="list-style-type: none"> CIS CSC 4.19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15 	1	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	<p>RS.MI-1: Incidents are contained</p> <ul style="list-style-type: none"> CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 	1	
		<p>RS.MI-2: Incidents are mitigated</p> <ul style="list-style-type: none"> CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 	1	
		<p>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks</p> <ul style="list-style-type: none"> CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 	1	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	<p>RS.IM-1: Response plans incorporate lessons learned</p> <ul style="list-style-type: none"> COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 	0	
		<p>RS.IM-2: Response strategies are updated</p> <ul style="list-style-type: none"> COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 	0	
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets	<p>RC.RP-1: Recovery plan is executed during or after a cybersecurity incident</p> <ul style="list-style-type: none"> CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 	1	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	<p>RC.IM-1: Recovery plans incorporate lessons learned</p> <ul style="list-style-type: none"> COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 	1	
		<p>RC.IM-2: Recovery strategies are updated</p> <ul style="list-style-type: none"> COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 	1	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	<p>RC.CO-1: Public relations are managed</p> <ul style="list-style-type: none"> COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4 	N/A	
		<p>RC.CO-2: Reputation is repaired after an incident</p> <ul style="list-style-type: none"> COBIT 5 MEOA03.02 ISO/IEC 27001:2013 Clause 7.4 	N/A	
		<p>RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and</p> <ul style="list-style-type: none"> COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4 	1	W kontekście internal