

Ćwiczenie 11 Konfigurowanie i testowanie kanałów IPsec

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.

ZADANIE 1 Weryfikacja poprawności komunikacji

1. Jeżeli wcześniej został zainstalowany pakiet PGP lub GPG, to należy go teraz „odinstalować”.
2. Według wskazówek prowadzącego, statycznie skonfigurować protokół TCP/IP na obu komputerach, na których realizowane będzie ćwiczenie. Komputery te umownie będą oznaczone w dalszym opisie ćwiczenia jako A i B.
3. Włączyć usługi IPsec.
4. Na obu komputerach uruchomić program MMC i do utworzonej konsoli dodać przystawkę **Monitor zabezpieczeń IP**. Zapisać plik konsoli na pulpicie pod nazwą `MONITOR_IPSEC_nr.komputera`. W konsoli `MONITOR_IPSEC_nr.komputera` otworzyć okno właściwości swojego komputera i ustawić czas odświeżania na 20 sekund.
5. Na obu komputerach zainstalować pakiet **WinPcap** i sniffer **Ethereal**. Uruchomić sniffer i zainicjować zbieranie pakietów:
 - W menu **Capture** wybrać funkcję **Start**.
 - Włączyć opcje:
Update list of packets in real time,
Automatic scrolling in live capture.
 - Zdefiniować filtr pakietów wpisując w polu **Filter**:
host adres_swojego_komputera and host adres_komputera_partnera
6. Wykorzystując program **ping**, na obu komputerach sprawdzić poprawność komunikacji z komputerem partnera. Obserwować jednocześnie zawartość okna programu **Ethereal** i kontenerów **Statystyka** w konsoli `MONITOR_IPSEC_nr.komputera` (dla trybu głównego i szybkiego). Co i dlaczego prezentowane jest w wymienionych oknach?

ZADANIE 2 Konfigurowanie kanału IPsec.

Ćwiczenie to powinno zostać zrealizowane na obu komputerach partnerskich.

Do konsoli `MONITOR_IPSEC_nr.komputera` dodać przystawkę **Zarządzanie zasadami zabezpieczeń IP (IP Security Policy Management)**. Przystawka ta ma umożliwić zarządzanie usługą na komputerze lokalnym

Zbudować zasadę reguł komunikacji IPsec:

1. W oknie konsoli, w menu podręcznym pozycji **Zasady zabezpieczeń IP w Komputer**

lokalny (*IP Security Policies on Local Machine*) wybrać funkcję **Utwórz zasadę zabezpieczeń IP** (*Create IP Security Policy*).

2. Korzystając z uruchomionego kreatora, nadać konstruowanej zasadzie nazwę ZASADA_IPSEC_nazwa.komputera, W trakcie pracy kreatora wyczyścić opcje **Włącz regułę odpowiedzi domyślnej** (*Activate the default response rule*) i **Edytuj właściwości** (*Edit properties*).

Zdefiniować reguły sterujące ruchem:

1. Otworzyć okno właściwości zasady ZASADA_IPSEC_nazwa.komputera.
2. W oknie zakładki **Reguły** (*Rules*) wyczyścić pole wyboru **Użyj kreatora dodawania** (*Use Add Wizard*), a następnie wybrać przycisk **Dodaj** (*Add*) aby utworzyć nową regułę.
3. W oknie zakładki **Lista filtrów IP** (*IP Filter List*) wybrać przycisk **Dodaj** (*Add*).
4. W oknie **Lista filtrów IP** (*IP Filter List*) wyczyścić pole wyboru **Użyj kreatora dodawania** (*Use Add Wizard*). W polu nazwy wpisać: DO_nazwa.komputera.partnera, a następnie wybrać przycisk **Dodaj** (*Add*) aby utworzyć nowy filtr.
5. W oknie zakładki **Adresy** (*Addresses*), w polu adresu źródłowego wybrać opcję **Mój adres IP** (*My IP Address*). W polu adresu docelowego wybrać opcję **Określony adres IP** (*A specific IP Address*) i podać adres komputera partnera. Zastanowić się, jakie znaczenie mają pozostałe opcje i kiedy się ich używa. Wyczyścić opcję **Dublowane** (*Mirrored*), by reguła nie dotyczyła pakietów przesyłanych z komputera partnera do naszego komputera.
6. W oknie zakładki **Protokół** (*Protocol*) wybrać opcję **Dowolny** (*Any*).
7. W oknie zakładki **Opis** (*Description*), tworzonemu filtrowi nadać nazwę DO_nazwa.komputera.partnera. Zatwierdzić wszystkie wprowadzone ustawienia.
8. W oknie zakładki **Lista filtrów IP** (*IP Filter List*) zaznaczyć pozycję filtra DO_nazwa.komputera.partnera.
9. Wybrać zakładkę **Ustawienia tunelowania** (*Tunnel Settings*) i w jej oknie podać adres komputera partnera.
10. Wybrać zakładkę **Akcja filtrowania** (*Filter Action*) i w jej oknie wyczyścić pole wyboru **Użyj kreatora dodawania** (*Use Add Wizard*), a następnie wybrać przycisk **Dodaj** (*Add*) aby zdefiniować akcję filtra.
11. W konfiguracji nowego filtra pozostawić aktywną opcję **Negocjuj protokół zabezpieczeń** (*Negotiate Security*) i zakreślić opcję **Akceptuj komunikację niezabezpieczoną ale zawsze odpowiadaj używając protokołu IPsec** (*Accept unsecured communication, but always respond using IPSec*).
12. Wybrać przycisk **Dodaj** (*Add*) i w kolejnym oknie dialogowym zaznaczyć opcję **Integralność i szyfrowanie**. Zatwierdzić zmiany powracając do okna zakładki **Akcja filtrowania** (*Filter Action*).
13. W oknie zakładki **Metody uwierzytelniania** (*Authentication Method*) należy wybrać metodę uwierzytelnienia przy zastosowaniu klucza wstępnego (*Preshared key*) i wpisać ustalone z partnerem hasło. Wybrana metoda powinna być jedyną w liście wybieranych metod.
14. Samodzielnie zdefiniować regułę kanału służącego do przekazywania danych w drugą stronę i nadać jej nazwę DO_nazwa.komputera.własnego.

Należy pamiętać, że każda reguła (filtr) określa sposób komunikowania się w jedną stronę. W związku z tym bardzo ważne jest np. rozróżnienie początku i końca kanału. Przemyśl to i podaj odpowiednie wartości w polach, które wypełniałeś realizując niniejsze ćwiczenia, a teraz musisz te same pola wypełnić samodzielnie.

Aktywować zdefiniowaną zasadę `ZASADA_IPSEC_nazwa.komputera` wybierając w jej menu podręcznym (okno główne konsoli) pozycję **Przypisz** (*Assign*).

ZADANIE 3 - Testowanie poprawności pracy kanału IPSec.

1. Zrestartować zbieranie pakietów w programie **Ethereal**. Na komputerze A, wykorzystując okno wiersza poleceń i program **ping** sprawdzić poprawność komunikacji z komputerem B. Program **ping** uruchomić dwukrotnie w odstępach około pół minuty. Jednocześnie obserwować zawartość okien programu **Ethereal** i kontenerów **Statystyka** w konsoli `MONITOR_IPSEC_nr.komputera` (dla trybu głównego i szybkiego).
2. Dokonać deaktywacji zdefiniowanych na obu komputerach zasad `ZASADA_IPSEC_nazwa.komputera` wybierając w ich menu podręcznym (okno główne konsoli) pozycję **Cofnij przypisanie** (*Un-assign*).
3. Dokonać aktywacji zdefiniowanych na obu komputerach zasad `ZASADA_IPSEC_nazwa.komputera` wybierając w ich menu podręcznym (okno główne konsoli) pozycję **Przypisz** (*Assign*).
4. Zrestartować zbieranie pakietów w programie **Ethereal**. Na komputerze B, wykorzystując okno wiersza poleceń i program **ping** sprawdzić poprawność komunikacji z komputerem A. Program **ping** uruchomić dwukrotnie w odstępach około pół minuty. Jednocześnie obserwować zawartość okien programu **Ethereal** i kontenerów **Statystyka** w konsoli `MONITOR_IPSEC_nr.komputera` (dla trybu głównego i szybkiego).

ZADANIE 4 - Wyłączanie zabezpieczeń IPSec.

1. Na komputerze A, w oknie wiersza poleceń wydać polecenie **net stop policyagent**.
2. Przy pomocy programu **ping** sprawdzić poprawność komunikacji na obu komputerach. Jednocześnie obserwować zawartość okien programu **Ethereal** i kontenerów **Statystyka** w konsoli `MONITOR_IPSEC_nr.komputera` (dla trybu głównego i szybkiego).
3. Na komputerze A, w oknie wiersza poleceń wydać polecenie **net start policyagent**.
4. Przy pomocy programu **ping** sprawdzić poprawność komunikacji na obu komputerach. Jednocześnie obserwować zawartość okien programu **Ethereal** i kontenerów **Statystyka** w konsoli `MONITOR_IPSEC_nr.komputera` (dla trybu głównego i szybkiego).
5. Dokonać deaktywacji zdefiniowanych na obu komputerach zasad `ZASADA_IPSEC_nazwa.komputera` wybierając w ich menu podręcznym (okno główne konsoli) pozycję **Cofnij przypisanie** (*Un-assign*). Usunąć wyżej wymienione zasady. Zatrzymać na obu komputerach zbieranie pakietów w programie **Ethereal**. Na obu komputerach, w oknie wiersza poleceń wydać polecenie **net stop policyagent**.
6. Wyłączyć usługi IPSec.
7. Skasować konsolę `MONITOR_IPSEC_nr.komputera`.