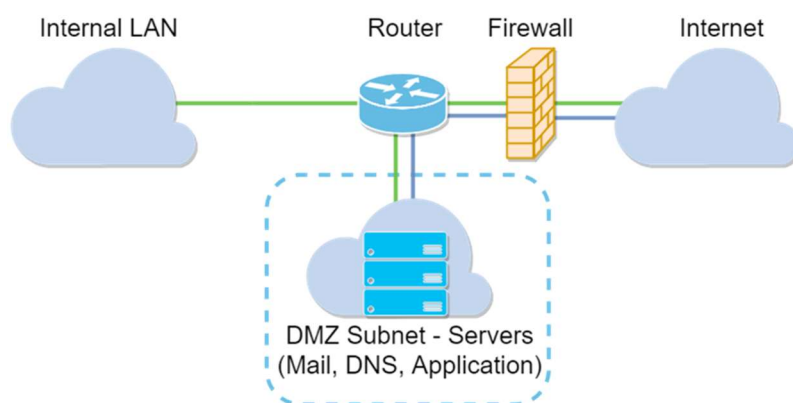


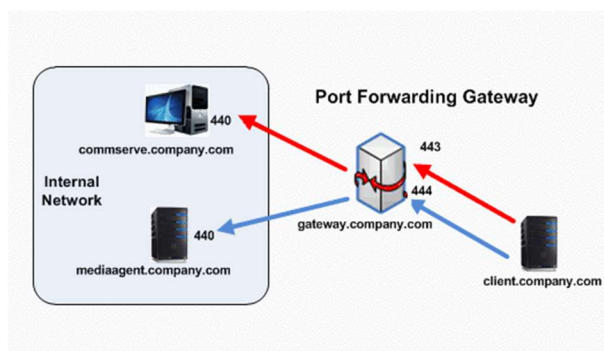
INSTRUKCJA ROUTER firewall, port forwarding

DMZ (ang. demilitarized zone) – strefa zdemilitaryzowana bądź ograniczonego zaufania – jest to wydzielany na zaporze sieciowej (ang. *firewall*) obszar sieci komputerowej nienależący ani do sieci wewnętrznej (tj. tej chronionej przez zaporę), ani do sieci zewnętrznej (tej przed zaporą; na ogół jest to Internet). W strefie zdemilitaryzowanej umieszczane są serwery „zwiększonego ryzyka włamania”, przede wszystkim serwery świadczące usługi użytkownikom sieci zewnętrznej, którym ze względów bezpieczeństwa nie umożliwia się dostępu do sieci wewnętrznej (najczęściej są to serwery WWW i FTP). W strefie zdemilitaryzowanej umieszczane są także te serwery usług świadczonych użytkownikom sieci wewnętrznej, które muszą kontaktować się z obszarem sieci zewnętrznej (serwery DNS, proxy, poczty i inne), oraz serwery monitorujące i reagujące na próby włamań IDS. W przypadku włamania na serwer znajdujący się w strefie DMZ intruz nadal nie ma możliwości dostania się do chronionego obszaru sieci wewnętrznej. Określenie „strefa demilitaryzowana” pochodzi z terminologii wojskowej i oznacza obszar buforowy pomiędzy wrogimi siłami.



©cisco.com

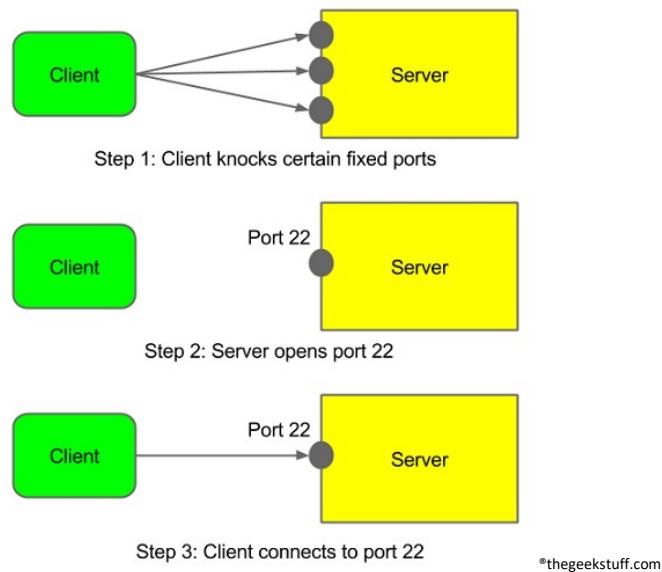
Przekierowanie portów (ang. port forwarding) – przekierowanie pakietów z Internetu, przychodzących na określony port serwera, do innego komputera w sieci lokalnej. Przekierowane mogą być protokoły TCP, UDP i inne. W zależności od implementacji i używanego narzędzia, przekierowanie pakietów następuje domyślnie na te same porty, do maszyny wewnątrz sieci lokalnej, bądź są one zmieniane na inne. Umożliwia komputerom spoza sieci wewnętrznej (LAN) połączyć się z komputerem stojącym za bramą (np. w strefie DMZ). Przekierowanie portów stosowane jest w razie konieczności łączenia się z zewnątrz z komputerami w sieci wewnętrznej (np. gdy użytkownik chce stworzyć serwer na swoim komputerze, podłączonym do sieci poprzez mechanizm maskarady). Jest to standardowa opcja dostępna w większości routerów.



©commvault.com

Port triggering – funkcjonalność pozwalająca na automatyczne przekierowanie danych portów jeśli router wykryje na nich chęć rozpoczęcia ruchu sieciowego. W przypadku braku ruchu na danych portach przez określony czas zostają one zamknięte.

Port knocking – metoda pozwalająca na nawiązanie zdalnego połączenia z usługami działającymi na komputerze, do którego dostęp został ograniczony np. za pomocą zapory sieciowej, umożliwiającą odróżniania prób połączeń, które powinny i nie powinny być zrealizowane. Z punktu widzenia klienta bez autoryzacji, na serwerze nie ma otwartych portów. Autoryzowany system, z którego ma nastąpić połączenie, wysyła serię pakietów na zamknięte porty maszyny docelowej. Pakiety te są ignorowane (pozostawione bez odpowiedzi), ale odpowiednie oprogramowanie śledzi przychodzące pakiety i jeśli pakiety z danego adresu IP układają się w zdefiniowaną dla pewnej usługi sekwencję, wówczas system zezwala na połączenie z nią z tego adresu IP.



WAŻNE !

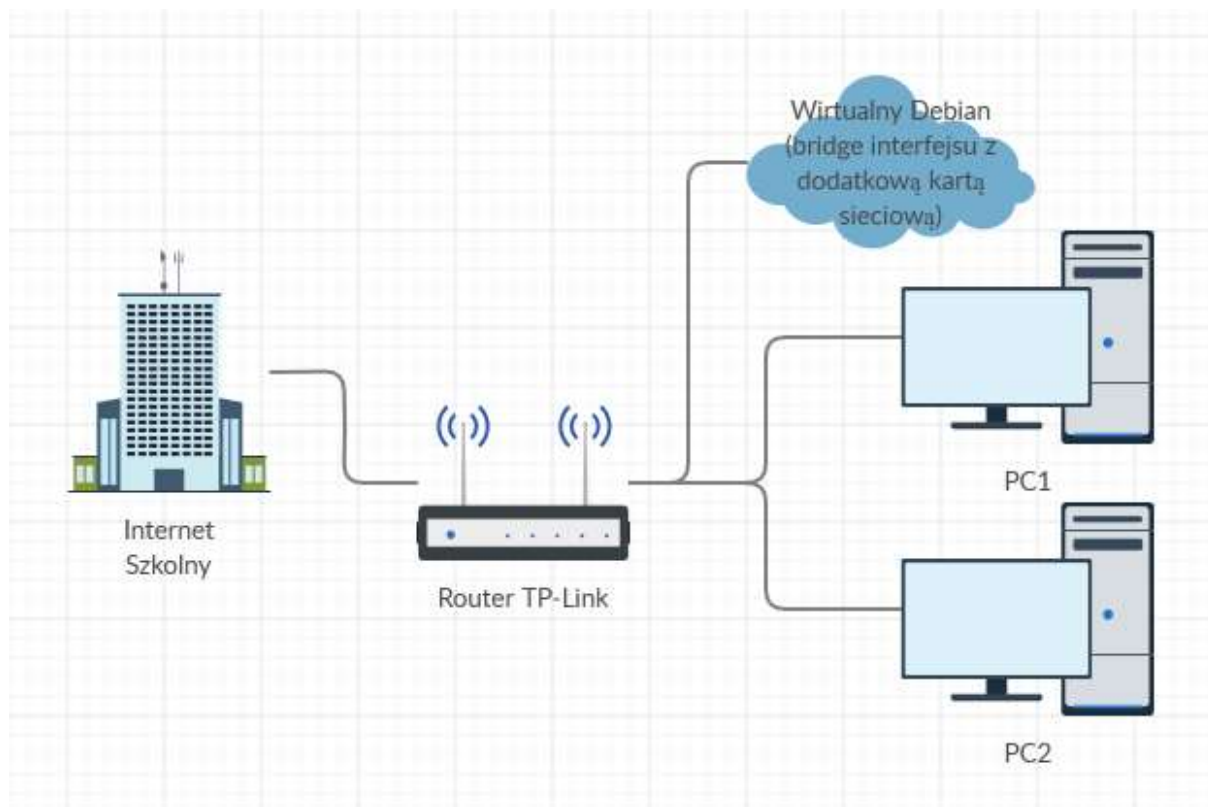
Telnet jest to standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala w architekturze klient-serwer.

UFW (ang. Uncomplicated Firewall) – program służący do tworzenia zapory sieciowej (Linux), prosty i skuteczny.

Apache to otwarty serwer HTTP dostępny dla wielu systemów operacyjnych.

WPROWADZENIE

Dzisiejsza instrukcja wymaga zainstalowania systemu Debian (bez GUI) na jednym z komputerów (wykorzystanie VMware bądź Virtualbox) które będą wykorzystywane w grupie. Poniżej schemat działania:



Podczas instalacji systemu Debian pamiętaj aby zainstalować jedynie podstawowe narzędzia bez wspomaganie GUI czy predefiniowanych serwerów. Po ukończeniu instalacji oraz pierwszym logowaniu opuść maszynę i w ustawieniach sieci zaznacz opcję bridge (wybierz niewykorzystaną kartę sieciową). Następnie włącz maszynę aktualizujemy wszystkie pakiety po czym przystępujemy do instalacji UFW oraz usługi HTTP.

UFW przykład

1	<code>apt-get install ufw</code>	Instalacja
2	<code>ufw app list</code>	Lista profili które można włączyć/wyłączyć
3	<code>ufw allow 'FTP'</code>	Zezwalamy aby profil (port) FTP został otwarty
4	<code>ufw status</code>	Pokazuje otwarte porty

APACHE przykład

1	<code>apt-get install apache2</code>	Instalacja
2	<code>systemctl status apache2</code>	Sprawdzenie czy usługa jest aktywna

Do celów testowych wykorzystamy stronę bazową serwera http z modyfikacją polegającą na edycji tekstu (dla udowodnienia działania usługi).

ZADANIA do wykonania

4. Skonfiguruj ruter według zaleceń. Wykonaj zrzuty ekranu potwierdzające wykonaną konfigurację routera. Zrzuty zapisz jako pliki graficzne na nośniku USB opisanym *EGZAMIN* w folderze *KONFIGURACJA-RUTERA*

UWAGA: ruter pracuje na ustawieniach fabrycznych zgodnie z dokumentacją, która jest dostępna w folderze RUTER na nośniku opisanym MATERIAŁY

- a) adres IP dla interfejsu LAN: 192.168.100.1/24
- b) serwer DHCP włączony, zakres adresów: 192.168.100.25 - 192.168.100.65
- c) adres 192.168.100.26 zarezerwowany dla interfejsu stacji roboczej, podłączonej do przełącznika
- d) adres IP interfejsu WAN: 10.10.10.2/28, brama 10.10.10.1
- e) serwer DNS dla interfejsu WAN: 8.8.8.8, drugi serwer DNS: 8.8.3.3, jeśli jest wymagany

ee.08 2020 czerwiec

Na systemie Debian zainstalowałeś UFW i Apache zgodnie z przykładami. Wpisując adres IP Debiana widzisz stronę powitalną usługi Apache (ze wszystkich urządzeń po stronie LAN). Naszym zadaniem jest aby Debian stał się serwerem również dla sieci wyżej (aby nauczyciel mógł wejść ze swojego komputera podpiętego do sieci szkolnej).

Jeżeli serwer http działa prawidłowo w sieci lokalnej to:

Musisz wykonać *port forwarding*, tak aby wszyscy wpisujący adres WAN Twojego routera w przeglądarce internetowej zobaczyli stronę powitalną Apache.

Na drugim PC (bez maszyny z Debianem), wykorzystaj pakiet XAMPP w identycznym celu jak wyżej tyle że w środowisku Windows 10.