Ściany Ogniowe w systemie Linux

Ściany ogniowe (firewalle) w systemie Linux to narzędzia służące do zarządzania ruchem sieciowym, które kontrolują, które połączenia są dozwolone, a które blokowane w oparciu o określone zasady bezpieczeństwa. W systemie Linux firewalle są kluczowym elementem w zapewnianiu bezpieczeństwa sieciowego, umożliwiając administratorom ochronę przed nieautoryzowanym dostępem oraz innymi zagrożeniami związanymi z siecią.

1. iptables:
Najbardziej popularnym narzędziem do zarządzania zaporami sieciowymi w systemie Linux jest **iptables**. Jest to narzędzie wbudowane w jądro systemu Linux, które pozwala na tworzenie i zarządzanie regułami filtracji pakietów. Iptables umożliwia definiowanie zasad dotyczących przychodzącego i wychodzącego ruchu sieciowego, na przykład poprzez określenie, które porty są otwarte, jakie protokoły mogą być używane, a także które adresy IP mogą mieć dostęp do zasobów systemu. Reguły w iptables są zazwyczaj zapisane w tabelach, które są podzielone na różne łańcuchy odpowiadające różnym etapom przetwarzania pakietów.

2. nftables:
nftables to nowsza i bardziej zaawansowana wersja narzędzia iptables, które zostało wprowadzone w jądrze Linux 3.13. Jest to system zarządzania zaporami, który zastępuje iptables, ip6tables, arptables oraz ebtables, umożliwiając jednolite zarządzanie różnymi typami ruchu w jednym narzędziu. Nftables oferuje bardziej zwięzłą składnię, lepszą wydajność oraz elastyczność w definiowaniu reguł, co czyni go preferowanym rozwiązaniem w nowszych dystrybucjach Linuksa. Nftables umożliwia łatwiejsze zarządzanie i bardziej złożoną konfigurację reguł, dzięki czemu jest bardziej skalowalny.

3. Firewalld:
Firewalld to narzędzie zapory sieciowej, które bazuje na iptables, ale oferuje bardziej przyjazny interfejs do zarządzania regułami zapory. Jest dostępne głównie w dystrybucjach takich jak CentOS, Fedora oraz RHEL. Firewalld działa na zasadzie stref, które definiują poziom zaufania dla różnych połączeń sieciowych. Każda strefa ma przypisane reguły dotyczące ruchu, co pozwala na łatwiejsze zarządzanie zaporą w porównaniu do iptables. Firewalld pozwala na dynamiczne dodawanie, usuwanie i modyfikowanie reguł bez konieczności restartowania zapory, co czyni go wygodnym narzędziem w środowiskach produkcyjnych.

4. UFW (Uncomplicated Firewall):
UFW to narzędzie zapory, które jest szczególnie popularne w dystrybucjach opartych na Debianie, takich jak Ubuntu. Jego celem jest zapewnienie prostoty konfiguracji zapory przy zachowaniu wysokiego poziomu bezpieczeństwa. UFW zapewnia łatwy sposób na tworzenie reguł filtracji pakietów za pomocą prostych poleceń. Dzięki temu jest to dobre rozwiązanie dla osób, które nie chcą zagłębiać się w szczegóły iptables, a potrzebują narzędzia do szybkiej konfiguracji zapory. UFW jest idealnym rozwiązaniem dla początkujących użytkowników Linuxa, którzy potrzebują prostych, ale skutecznych narzędzi zabezpieczających.

5. SELinux i AppArmor:
Choć **SELinux** (Security-Enhanced Linux) i **AppArmor** nie są zaporami sieciowymi w tradycyjnym sensie, to również pełnią istotną rolę w bezpieczeństwie systemu Linux, zwłaszcza w kontekście ochrony aplikacji i procesów przed nieautoryzowanym dostępem. SELinux to mechanizm kontroli dostępu oparty na politykach, który może ograniczać, do jakich zasobów mogą uzyskać dostęp aplikacje w systemie. Z kolei AppArmor oferuje podobną funkcjonalność, pozwalając na tworzenie profili bezpieczeństwa dla aplikacji i usług. Oba narzędzia współpracują z zaporami, aby zapewnić wielowarstwową ochronę

systemu.

6. Zastosowanie ścian ogniowych w praktyce:
W kontekście praktycznym, zapory ogniowe w systemie Linux pełnią rolę pierwszej linii obrony przed atakami z sieci. Mogą być używane do blokowania nieautoryzowanego dostępu do systemu, ochrony przed atakami typu DoS (Denial of Service) oraz kontrolowania ruchu wychodzącego z systemu. W środowiskach produkcyjnych często stosuje się połączenie kilku narzędzi, takich jak firewalld lub iptables wraz z SELinux lub AppArmor, aby zapewnić kompleksową ochronę systemu przed zagrożeniami z sieci.

Zarządzanie zaporami sieciowymi w systemie Linux jest kluczowym elementem zapewnienia bezpieczeństwa i integralności systemu. Odpowiednia konfiguracja zapory ogniowej może znacząco zwiększyć odporność systemu na ataki z sieci, jednocześnie umożliwiając elastyczną kontrolę nad dostępem do zasobów systemowych.

Należy zacząć od świeżej instalacji posiadanej dystrybucji Linuxa (poniższe przykłady bazują na dystrybucji RedHat 3.0.3). Im mniej oprogramowania zostanie zainstalowane tym mniej będzie w nim dziur, tylnych wejść i / lub błędów wprowadzających do naszego systemu problem bezpieczeństwa, więc dobrze jest zainstalować jedynie minimalny zestaw aplikacji.

Należy użyć stabilnego jądra. Poniżej przedstawiona jest dokumentacja podstawowych ustawień (dla wersji 2.0.14) [1].

Oto są sieciowe ustawienia, które poznajemy wykonując komendę make config

1. Under General setup
    1. Turn Networking Support ON
2. Under Networking Options
    1. Turn Network firewalls ON
    2. Turn TCP/IP Networking ON

    3. Turn IP forwarding/gatewaying OFF (UNLESS you wish to use IP filtering)
    4. Turn IP Firewalling ON
    5. Turn IP firewall packet loggin ON (this is not required but it is a good idea)
    6. Turn IP: masquerading OFF (I am not covering this subject here.)
    7. Turn IP: accounting ON
    8. Turn IP: tunneling OFF
    9. Turn IP: aliasing OFF
    10. Turn IP: PC/TCP compatibility mode OFF
    11. Turn IP: Reverse ARP OFF
    12. Turn Drop source routed frames ON
3. Under Network device support
    1. Turn Network device support ON
    2. Turn Dummy net driver support ON
    3. Turn Ethernet (10 or 100Mbit) ON
    4. Select your network card

Teraz możemy dokonać rekompilacji i reinstalacji jądra oraz zrestartować system. Nasza karta/y sieciowa/e powinna pojawić się w trakcie procedury startowej.

---

[1] R. Ziegler „Linux. Firewalls“