Systemy firewall nowej generacji

Właściwa ochrona systemów IT wymaga, aby zabezpieczenia były dostosowane do zmian w architekturze sieci i nowych zagrożeń. Tradycyjne systemy zabezpieczeń, które spełniały wszystkie oczekiwania i zapewniały bezpieczeństwo jeszcze kilka lat temu stają się obecnie nieadekwatne zarówno pod względem rosnących potrzeb funkcjonalnych jak i zapewnianego poziomu ochrony. Standardy bezpieczeństwa obowiązujące 3-4 lata temu, tj.: system firewall filtrującym ruch na podstawie portu sieciowego i adresu oraz system antywirusowy usuwającym złośliwy kod, w dobie zagrożeń takich jak ataki "zero-day" oraz "APT" stają się zdecydowanie przestarzałe.

Bezpieczeństwo

Wdrażane przez nas rozwiązania firewalli nowej generacji (NGFW) zapewniają ochronę sieci przed współczesnymi zagrożeniami: realizują filtrację danych dla różnorodnych aplikacji Web.

Pozwalają np. na zablokowanie dostępu do wybranych komunikatorów internetowych oraz ograniczenie przepustowości (ale nie całkowitą blokadę) takich aplikacji jak Facebook czy YouTube.

Oferowane przez nas systemy zabezpieczeń chronią użytkowników przed złośliwym oprogramowaniem typu Trojan oraz pozwalają na wykrycie tego typu oprogramowania - jeśli znajdzie się ono w sieci.

Wysoka wydajność

Wymagania wydajnościowe względem współczesnych systemów bezpieczeństwa rosną z każdym rokiem, wynika to z kilku względów:

- wzrostu przepustowości łącz internetowych,
- wzrostu zapotrzebowania na filtrację, nie tylko na styku LAN-Internet, ale także pomiędzy poszczególnymi segmentami LAN,
- konieczności filtrowania nie tylko nagłówków ale i całej zawartości pakietów,
- analizy i filtrowania ruchu zaszyfrowanego.

Oferowane przez nas systemy zapewniają pełną filtrację ruchu dla przepustowości: 100 Mbps, 1 Gbps a nawet ponad 10 Gbps - w zależności od potrzeb klienta.

PRZETESTUJ!

Proponujemy darmowe, testowe wdrożenie systemu NGF, pozwala ono na zapoznanie się z technolgią nowoczesnych zabezpieczeń. Testowany system może być wdrożony w różnych konfiguracjach, w tym także w sposób całkowicie "nieinwazyjny" dla reszty środowiska (nie jest wymagana jakakolwiek rekonfiguracja istniejących systemów sieciowych). Często też nawet kilkudniowe testy prowadzą do wykrycia i eliminacji złośliwego oprogramowania (bot, trojan, wirus) ukrytego na komputerach użytkowników.

www.cc.com.pl

Interesujący fakt #1

Ataki "zero-day" bazują na złośliwym kodzie wykorzystującym nowo wykryte luki bezpieczeństwa (np. w systemach Windows lub programach takich jak Adobe Acrobat). Bazowanie przez hackerów na najnowszych błędach powoduje odporność złośliwego kodu na skanowanie antywirusowe.

Interesujący fakt #2

"APT" czyli "Advanced Persistent Threat" to oprogramowanie infekujące sieć lokalną poprzez Internet, pozostaje w niej niewykryte przez dłuższy czas i realizuje zadania kradzieży, modyfikacji i niszczenia danych, a także wykorzystuje przejęte komputery n.p. do rozsyłania spamu czy też jako "stacje przesiadkowe" do prowadzenia dalszych ataków.

Interesujący fakt #3

Ponad 70% aplikacji internetowych jest nierozpoznawana przez tradycyjne systemy firewalli sieciowych, gdyż większość programów on-line działa na bazie protokołów HTTP i HTTPS. Standardowy system firewall nie odróżnia ruchu sieciowego generowanego n.p. przez YouTube, Facebook czy Gmail i tym samym nie pozwala na odrębne traktowanie tych aplikacji w regułach filtracji ruchu.

Interesujący fakt #4

W systemach UTM inspekcja ruchu aplikacyjnego dokonywana jest w wielu modułach (np. IPS, antywirus, itd.), które wzajemnie przekazują sobie dane. Powoduje to znaczne obniżenie wydajności - nawet do 95% w stosunku do zadeklarowanej przez producenta wydajności systemu.

Interesujący fakt #5

Identyfikacja nieznanego wrogiego kodu (malware) poprzez bezpośrednią obserwację zachowania w wirtualnym środowisku nosi nazwę „sandbox". Technika ta polega na uruchamianiu ściągniętego przez użytkowników kodu (w sposób zautomatyzowany i przeźroczysty dla użytkownika w kontrolowanym i całkowicie odseparowanym środowisku). Technika ta gwarantuje bardzo wysokie prawdopodobieństwo wykrycia nieznanych nowych wirusów, wymaga jednak od systemu firewall znacznej mocy przetwarzania.

Producenci:
Check Point, Palo Alto Networks, Websense

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: office@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
http://www.cc.com.pl/

Kontakt:
Dział Techniczny: tech@cc.com.pl
Dział Handlowy: sales@cc.com.pl