# Systemy firewall nowej generacji

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

## Ochrona przed współczesnymi zagrożeniami

Wdrażane przez nas rozwiązania firewalli nowej generacji (NGF) zapewniają ochronę sieci przed współczesnymi zagrożeniami: realizują filtrację danych dla różnorodnych aplikacji Web.
Pozwala to m.in. na zablokowanie dostępu do wybranych komunikatorów internetowych oraz na ograniczenie przepustowości (ale nie całkowitą blokadę) takich aplikacji jak Facebook czy YouTube.
Oferowane przez nas systemy zabezpieczeń chronią użytkowników przed złośliwym oprogramowaniem typu: ansomware, Bot, APT 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 oraz przepustowości LAN,
- wzrostu zapotrzebowania na filtrację, nie tylko na styku LAN-Internet, ale także pomiędzy poszczególnymi segmentami sieci lokalnej,
- 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: od 0,5 Gbps, poprzez systemy średniej skali z przepustowością 1 Gbps do 10 Gbps, do systemów o przepustowości powyżej 10 Gbps, aż do 200 Gbps - w zależności od potrzeb klienta.

## Centrum danych, chmura prywatna i publiczna

Współczesne systemy firewall stają się częścią bardziej złożonego ekosystemu bezpieczeństwa obejmującego zwirtualizowane serwery, a także usługi chmurowe. Rozwiązania, które oferujemy pozwalają na pełną integrację z platformami wirtualizacyjnymi, takimi jak np.: VMware, VMware NSX, Hyper-V, VirtualBox i innymi; funkcjonują w chmurze, w zależności od potrzeb - zarówno publicznej jak i prywatnej; pozwalają też na ochronę rozwiązań chmurowych.

## PRZETESTUJ!

**Proponujemy darmowe, testowe wdrożenie systemu NGF, pozwala ono na zapoznanie się z technolgią nowoczesnych zabezpieczeń. Często nawet kilkudniowe testy prowadzą do wykrycia i eliminacji złośliwego oprogramowania (bot, trojan, wirus) ukrytego na komputerach użytkowników.**

## CC oferuje

W dziedzinie rozwiązań firewall oferujemy nie tylko dostawy sprzętu, ale także pełną gamę usług: prowadzimy analizę potrzeb klientów, projektujemy sieci i serwerownie, realizujemy testy oraz diagnostykę istniejącej infrastruktury, wykonujemy częściowe lub pełne migracje rozwiązań firewall, wdrażamy i konfigurujemy nowy sprzęt, prowadzimy nadzór oraz utrzymanie w trybie 24x7, a także realizujemy szkolenia warsztatowe. Wszystkie usługi wykonywane są przez naszych pracowników posiadających certyfikaty inżynierów danego producenta - posiadamy i utrzymujemy aktualne certyfikacje wszystkich kluczowych, wymienionych niżej dostawców rozwiązań bezpieczeństwa.


- "APT" czyli "Advanced Persistent Threat" to oprogramowanie infekujące sieć lokalną poprzez internet, pozostające w niej niewykryte przez dłuższy czas i realizujące zadania kradzieży, modyfikacji i niszczenia danych, a także wykorzystujące przejęte komputery np. do rozsyłania spamu czy też jako "stacji przesiadkowej" do prowadzenia dalszych ataków.

- Ponad 70% aplikacji internetowych jest nierozpoznawanych przez tradycyjne systemy Firewalli sieciowych, gdyż większość z nich działa na bazie protokołów HTTP i HTTPS. Standardowy system firewall nie odróżnia ruchu sieciowego generowanego np. przez Youtube, Facebook czy Google Mail i tym samym nie pozwala na odrębne traktowanie tych aplikacji w regułach filtracji ruchu.

- 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 prawdo-podobieństwo wykrycia nieznanych nowych wirusów, wymaga jednak od systemu firewall znacznej mocy przetwarzania.

**Producenci:**
**Palo Alto Networks, Check Point Technologies, Fortinet, Juniper Networks, Forcepoint**

paloalto · Check Point · FORTINET · JUNIPER NETWORKS · FORCEPOINT

**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: sales@cc.com.pl

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

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