

Connectra firmy Check Point

Brama zabezpieczająca

CECHY PRODUKTU:

- bezpieczny dostęp przez sieć Web
- zintegrowane zabezpieczenia serwerów
- inteligentne zabezpieczenia zdalnych węzłów
- bezpieczny dostęp do zasobów ekstranet z wykorzystaniem technologii One-click SSL

ZALETY PRODUKTU

- umożliwia zdalny dostęp poprzez przeglądarkę WWW
- zwiększa mobilność i produktywność zdalnych pracowników,
- chroni serwery i aplikacje przed zewnętrznymi atakami przez sieć SSL VPN
- zapobiega kradzieży tożsamości, haseł i danych ze zdalnych węzłów
- ułatwia wdrażanie aplikacji ekstranetowych



TWOJE WYZWANIA

Wraz z rosnącą różnorodnością i zwiększającą się mobilnością siły roboczej, kluczowym wyzwaniem dla wielu firm stało się umożliwienie łatwego dostępu do zasobów firmy z dowolnego miejsca. Rozwiązanie zdalnego dostępu typu SSL VPN za pomocą przeglądarki WWW okazało się wygodnym sposobem umożliwienia takiego dostępu użytkownikom i partnerom biznesowym. Organizacje, umożliwiając użytkownikom łączenie się z siecią przy użyciu przeglądarek, ułatwiają dostęp zdalnym użytkownikom, zmniejszając jednocześnie koszty takiego dostępu. Jednak samo korzystanie ze zdalnego dostępu poprzez sieć VPN opartą o protokół SSL nie czyni jeszcze takiego połączenia bezpiecznym.

Przykładowo zezwolenie na dostęp przez przeglądarkę oznacza, że użytkownik korzysta z zasobów wewnętrznej sieci firmy, łącząc się z komputerów nie zarządzanych przez firmę, znajdujących się w domu lub kafejce na lotnisku. Te zdalne węzły mogą być słabo lub wcale nie zabezpieczone przed zagrożeniami, co gorsze mogą mieć zainstalowane niebezpieczne oprogramowanie typu spyware lub malware. Bardziej istotne jest jednak bezpieczeństwo firmowych serwerów i aplikacji. Brak możliwości kontrolowania bezpieczeństwa zdalnych węzłów oznacza narażenie wewnętrznych serwerów i aplikacji na zagrożenia ze strony niezabezpieczonych węzłów.

Mimo iż rozwiązanie SSL VPN umożliwia użytkownikom łatwy dostęp do firmowej sieci, to bez zastosowania odpowiednich zabezpieczeń w samej sieci, rozwiązanie to naraża ją na nowe niebezpieczeństwa.

NASZE ROZWIĄZANIE

Urządzenie Connectra firmy Check Point jest kompletnym urządzeniem zabezpieczającym sieć Web, które dostarcza w jednym produkcie zarówno rozwiązania SSL VPN jak i mechanizmy zabezpieczeń sieci. Połączenie prostego, zdalnego dostępu i zabezpieczeń w jednym produkcie pozwala firmom wdrażać rozwiązania SSL VPN bezpiecznie i z zaufa-

niem z jakim zwykło się wdrażać rozwiązania firmy Check Point – najbardziej wiarygodnego dostawcy inteligentnych rozwiązań zabezpieczających.

Urządzenie Connectra umożliwia prosty dostęp w połączeniu z bezkonkurencyjnym poziomem bezpieczeństwa.

- **Bezpečny dostęp przez sieć WWW** – umożliwia zdalnym użytkownikom bezpieczny dostęp do aplikacji webowych oraz typu klient-serwer poprzez przeglądarkę WWW.
- **Zintegrowane zabezpieczenia serwerów** – technologie Application Intelligence oraz Web Intelligence chronią serwery przed atakami.
- **Inteligentne zabezpieczenie zdalnych węzłów** – kontroluje obecność oprogramowania typu spyware na zdalnych węzłach oraz przydziela prawa dostępu w zależności od poziomu bezpieczeństwa i wiarygodności urządzeń w nich funkcjonujących.
- **Ekstranet w technologii One-Click SSL** – umożliwia szybką i łatwą instalację bez potrzeby skomplikowanej konfiguracji serwera lub sieci.

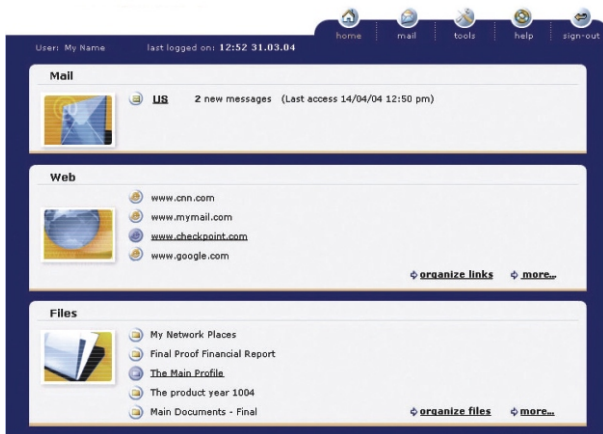
CECHY PRODUKTU

Bezpečny dostęp przez sieć WWW

Urządzenie Connectra umożliwia bezpieczny dostęp poprzez protokół SSL zarówno z poziomu sieci, jak i poprzez przeglądarkę WWW. Connectra to brama wykorzystywana przez zdalnych użytkowników do korzystania z zasobów firmowej sieci. Poprzez zintegrowany portal użytkownicy mają dostęp do aplikacji i zasobów webowych, współdzielenia plików oraz poczty. Dodatkowo firma może dostosować wygląd portalu umożliwiając np. obsługę wielu języków.



Connectra to kompletne urządzenie zabezpieczające sieć oraz umożliwiające bezpieczny zdalny dostęp.



Portal Connectra Web umożliwia zdalnym użytkownikom wygodne przeglądanie poczty, uruchamianie aplikacji webowych oraz dostęp do serwerów z zasobami plikowymi poprzez przeglądarkę internetową.

Dla użytkowników aplikacji klient-serwer dostarczany jest mechanizm SSL Network Extender umożliwiający bezpieczny dostęp do firmowej sieci poprzez technologię Web. Jest to wtyczka (plug-in) do przeglądarek WWW, która umożliwia tunelowanie poprzez protokół SSL ruchu aplikacyjnego pochodzącego ze zdalnych węzłów. Obsługiwane są dowolne aplikacje IP, w tym korzystające zarówno z protokołu TCP jak i UDP, bez konieczności ich skomplikowanej rekonfiguracji. Rozwiązanie to wspiera nawet aplikacje FTP oraz VoIP, mimo sprawianych przez nie problemów związanych z wykorzystywaniem dynamicznych portów.

Zintegrowane zabezpieczenie serwerów

W przeciwieństwie do innych rozwiązań dostępnych na rynku, Connectra posiada wbudowane, pro aktywne zabezpieczenia chroniące wewnętrzne serwery i aplikacje przed atakami. Zintegrowane technologie Web Intelligence oraz Application Intelligence

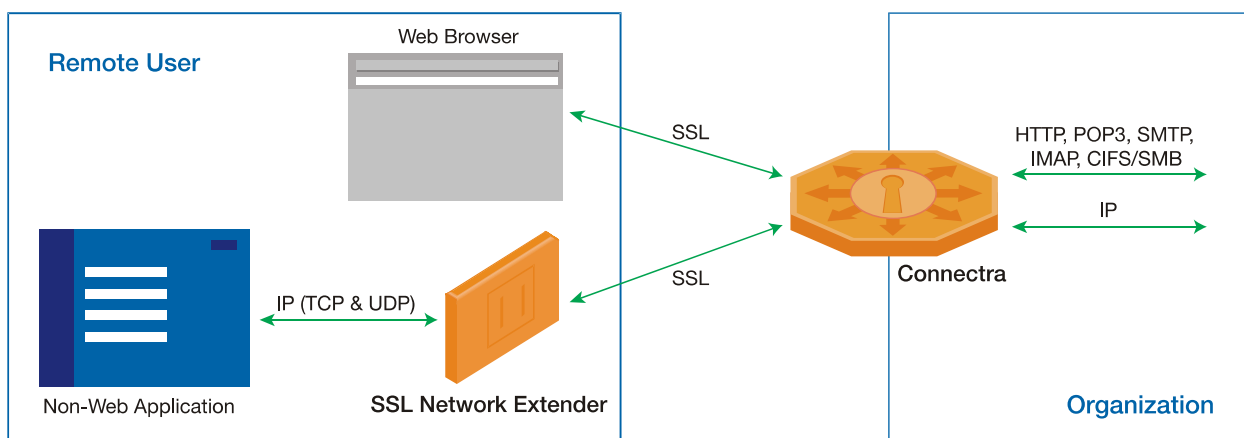
zapewniają ochronę przed atakami przeprowadzanymi poprzez SSL typu directory traversal, SQL injection oraz robakami internetowymi. Ochrona przed atakami sieciowymi pochodzącymi z węzłów zdalnych korzystających z dostępu poprzez SSL z poziomu sieci zapewniana jest przez mechanizm SmartDefense. Zawarta roczna subskrypcja na usługi SmartDefense sprawia, że zabezpieczenia pozostają cały czas aktualne.

Inteligentne zabezpieczenia zdalnych węzłów

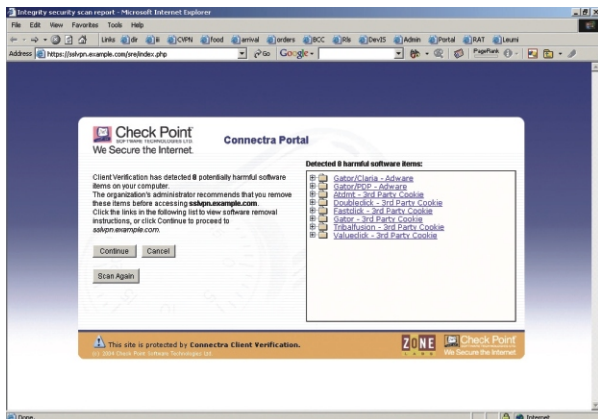
Urządzenie Connectra dostarcza zdalnym węzłom bogatego zbioru funkcji, które pozwalają przystosować go do różnych scenariuszy dostępu do sieci. Connectra umożliwia dostosowanie praw dostępu zdalnego użytkownika w zależności od wiarygodności i bezpieczeństwa zdalnego węzła.

Zawsze aktualnym wyzwaniem dotyczącym bezpieczeństwa jest uniemożliwienie zainstalowania na zdalnych węzłach złośliwych procesów, narzędzi typu keystroke loggers, koni trojańskich. W celu zapewnienia bezpieczeństwa danych, pakiet Integrity Clientless Security skanuje system zdalnego węzła (z poziomu przeglądarki użytkownika) w poszukiwaniu złośliwych procesów. Oprogramowanie to, dostarczane przez Zone Labs (firma Check Point), jest uznawane za wiodące na rynku rozwiązanie zabezpieczające odległe węzły.

Dzięki pakietowi Integrity Clientless Security administratorzy otrzymują możliwość sprawdzania wielu różnych rodzajów procesów tj.: keystroke loggers, konie trojańskie, robaki, oprogramowanie reklamowe (adware), wtyczki przeglądarki WWW, programy typu dialer, ciasteczka (cookies) oraz innego niepożądanego oprogramowania. Connectra zapobiega kradzieży tożsamości, haseł oraz utracie danych, zatrzymując złośliwe procesy i narzucając podstawowe wymagania bezpieczeństwa jeszcze przed nadaniem praw dostępu do SSL VPN.



Urządzenie Connectra firmy Check Point umożliwia dostęp poprzez sieć Web do poczty, współdzielenia plików oraz zasobów sieci przy wykorzystaniu portalu Connectra Web. Wtyczka przeglądarki WWW SSL Network Extender pozwala na zdalny dostęp do dowolnej aplikacji IP.



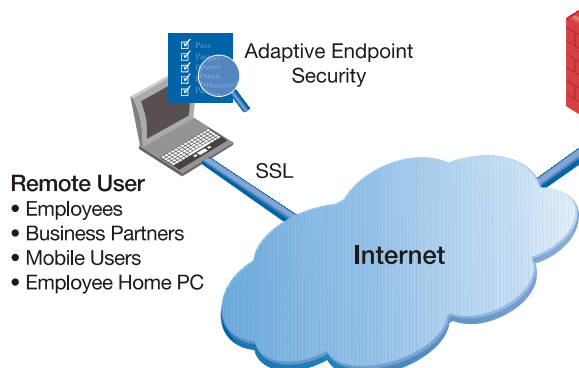
Pakiet Integrity Clientless Security wyszukuje złośliwe procesy działające na zdalnych węzłach oraz narzuca podstawowe wymagania bezpieczeństwa jeszcze przed zezwoleniem na dostęp do sieci.

Zasoby firmy mają różny poziom „wrażliwości”. Z pomocą urządzenie Connectra dostęp do tych zasobów budowany jest w oparciu o poziom wiarygodności zdalnego węzła oraz użytkownika. Na przykład, niektóre zasoby mogą mieć przypisany wysoki poziom ochrony i dostęp do nich będzie możliwy tylko wówczas, gdy zdalny węzeł umożliwi mocne uwierzytelnianie (np. uwierzytelnianie z użyciem tokena).

Inteligentna ochrona zdalnych węzłów realizowana przez Connectra umożliwi zabezpieczenie oparte na wiarygodności samego węzła oraz wiarygodności użytkownika.

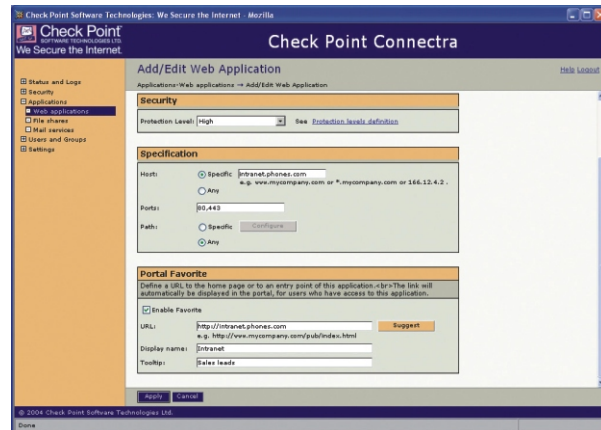
Ekstranet w technologii One-Click SSL

W przeszłości firmy, aby umożliwić dostęp swoim partnerom biznesowym do współdzielonych zasobów sieci, musiały konfigurować w tym celu pojedyncze serwery lub tworzyć specjalne strefy ekstranetu. Technologia One-Click SSL Extranet dostarcza znacznie prostszą strukturę i funkcje umożliwiające bezpieczny zdalny dostęp partnerom biznesowym. Użytkownicy ekstranetu korzystający ze zintegrowanego portalu mają dostęp poprzez sieć Web do współdzielonych zasobów firmy. Poprzez połączenie dostępu do aplikacji, serwerów i innych zasobów Connectra automatycznie buduje unikatowy portal Web dla określonych grup użytkowników ekstranetu. Jest to zdecydowanie prostsze rozwiązanie niż konfigurowanie pojedynczych serwerów dla zdalnego dostępu lub budowanie specjalnych stref ekstranetu.



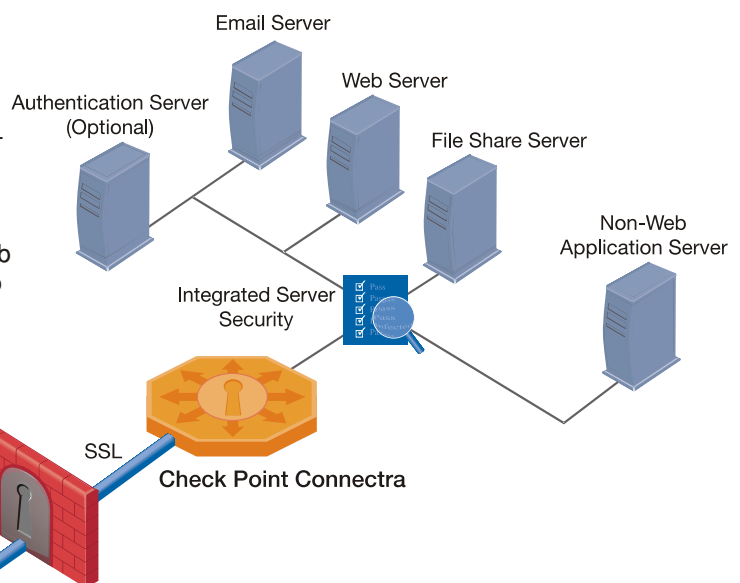
Proste wdrażanie i zarządzanie

Connectra, jako niezależne rozwiązanie, które można wdrożyć w sieci DMZ lub w zaufanej sieci LAN, jest rozwiązaniem prostym zarówno w instalacji, jak i w zarządzaniu. Intuicyjny, webowy interfejs administracyjny ułatwia definiowanie użytkowników, grup, aplikacji i zasobów, poziomów kontroli bezpieczeństwa na zdalnych węzłach oraz praw dostępu.



Intuicyjny, webowy interfejs administracyjny pozwala na szybkie zdefiniowanie zasobów i aplikacji. Przypisanie do zasobu określonego poziomu zabezpieczeń narzuca ustalone wymagania zabezpieczeń zdalnego węzła zanim jeszcze nadany zostanie dostęp do tego zasobu.

W przypadku wdrażania rozwiązania w środowisku, gdzie istnieje już baza danych uwierzytelniania, Connectra może integrować się z bazami takich rozwiązań jak LDAP, RADIUS, SecureID/ACE oraz FireWall-1 firmy Check Point. Connectra zawiera również wewnętrzną bazę danych dla tych firm, które nie posiadają jeszcze żadnej bazy danych uwierzytelniania.



Connectra firmy Check Point w prosty sposób umożliwia bezpieczny, zdalny dostęp do sieci firmy pracownikom i partnerom biznesowym. Rozwiązanie to łączy w sobie łatwy dostęp do zasobów poprzez przeglądarkę ze zintegrowanymi zabezpieczeniami dostępu przez sieć Web.

Dostęp poprzez Web

Bezpieczny dostęp

- SSL v.3, TLS
- RC4(128), 3DES, AES

Portal Connectra Web

- Web: linki statyczne, dynamiczne, względne, skrypty JavaScript i Vbscript.
- Opcje dostępu do poczty:
 1. zintegrowany interfejs Web do serwerów pocztowych IMAP
 2. natywne klienckie programy pocztowe (POP3, SMTP)
 3. SSL Outlook Web Access
- Współdzieleni plików: SMB/CIFS Windows, zwykłe przeglądanie poprzez Eksplorator Windows.
- Języki: angielski, francuski, włoski, niemiecki, hiszpański, chiński (tradycyjny i uproszczony), japoński.
- Obsługiwane przeglądarki: Internet Explorer 5.5+, Mozilla, Netscape 6+, Safari.

SSL Network Extender*

- Wtyczka ActiveX.
- Obsługiwane aplikacje: dowolna aplikacja IP (TCP i UDP), FTP, TFTP, Citrix, Telnet, rlogin, TN3270, VoIP, IMAP, POP, SMTP i inne.
- Obsługuje ruch w trybach Office Mode, split-tunnel lub route-all.
- Obsługiwane systemy operacyjne: Windows2K, XP

* dostępny w III kwartale 2004.

Zintegrowane zabezpieczenia serwerów

Ochrona przed atakami z sieci

Web Intelligence™: ochrona przed złośliwym kodem przekazywanym poprzez aplikacje webowe, robakami, różnorodnymi atakami jak np. Cross Site Scripting, przepełnienie bufora, SQL injection, Command injection, directory traversal oraz przeglądanie kodu HTTP.

Ochrona przed atakami z poziomu aplikacji

SmartDefence™* (ruch poprzez SSL Network Extender): wykorzystując Stateful Inspection™ oraz Application Intelligence™ aktywnie chroni firmy przed atakami zarówno na sieć jak i na aplikacje.

Uaktualnienia

Serwis SmartDefence™ przez cały rok (zawiera uaktualnienia SmartDefence™ oraz Web Intelligence™)

Ochrona przed ciasteczkami (cookies)

Ciasteczka są zabezpieczane i udostępniane poprzez bramę (gateway).

Automatyczny limit czasowy

Konfigurowany wstępnie lub ustawiany niestandardowo automatyczny limit czasowy sesji SSL VPN.

Inteligentne zabezpieczenia węzłów

Integrity Clientless Security™ (opcjonalnie)

- Wtyczka ActiveX.
- Kontrola oprogramowania typu malware: Keystroke loggers, konie trojańskie, robaki, oprogramowanie reklamowe (adware), wtyczki przeglądarek WWW, programy typu dialer, ciasteczka i inne niepożądane programy.
- Raportowanie: raportowanie zgodności z przyjętą polityką bezpieczeństwa przedstawianie niespełnionych przez użytkowników końcowych warunków bezpieczeństwa.

- Porady oraz odsyłacze do zasobów, które umożliwiają nowym użytkownikom uzyskanie statusu pełnoprawnych użytkowników sieci, spełniających warunki przyjętej w firmie polityki.
- Różne opcje działania: narzucenie zgodności z polityką bezpieczeństwa i zablokowanie dostępu, ostrzeżenia bez narzucania polityki lub wyłączenie skanowania węzłów.

Dynamiczne autoryzacja

- Nadawanie uprawnień dostępu to zasobów w oparciu o stopień autoryzacji.

Cechy urządzenia

	Connectra 1000: średniej klasy wdrożenia	Connectra 2000: wdrożenia klasy Enterprise	Connectra 6000: wdrożenia klasy Enterprise i wyższej
Licencje użytkowników	50,100,250	100,250, nieograniczona	250,500, nieograniczona
Maks.liczba użytkowników	250	Nieograniczona	Nieograniczona
Nadmiarowy zasilacz	Nie	Opcjonalnie	Tak
System operacyjny	SecurePlatform™ firmy Check Point		
Audyt i dzienniki (logs)	Zdarzenia administracyjne, zdarzenia użytkownika; eksport do SmartCenter Server		
Kopia zapasowa	manualna, automatyczna, przechowywana lokalnie/zdalnie		
Interfejsy	2 x 10/100/1000 Mbps Ethernet		
Wysokość	1.68"/4.2 cm (1 jednostka)		
Długość	17.61"/44.7 cm		
Głębokość	27"/68.3 cm		
Waga	35 funtów/15.9 kg		
Moc	100-220 V - 50/60 Hz		

Dystrybucja w Polsce:

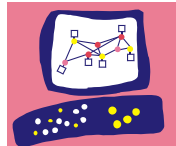


CLICO Sp. z o.o.
30-063 Kraków, Al. 3-go Maja 7
tel. (12) 632-51-66
tel. (12) 292-75-22 ... 25
fax (12) 632-36-98
e-mail: support@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-555 Katowice, ul. Rolna 43
tel. (32) 203-92-35
tel. (32) 609-80-50
tel. (32) 609-80-51
fax (32) 203-92-24
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
03-738 Warszawa, ul. Kijowska 1
tel. (22) 518-02-70...72
fax (22) 518-02-73
e-mail: warszawa@clico.pl

Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

©2004 Check Point Software Technologies Ltd.

Wszystkie prawa zastrzeżone. Check Point, logo firmy Check Point, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 SmallOffice, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECTXL, IQ Engine, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SVN, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Gard, VPN-1 Net, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 SmallOffice, oraz VPN-1 VSX są znakami handlowymi lub zastrzeżonymi znakami handlowymi firmy Check Point Software Technologies Ltd. oraz jej filii. Wszystkie inne nazwy produktów użyte w tym dokumencie są znakami handlowymi lub zastrzeżonymi znakami handlowymi ich prawowitych właścicieli. Produkty opisane w niniejszym dokumencie są chronione przez Patenty USA nr 5 606 668 i 5 835 726 oraz mogą być chronione przez inne patenty USA, patenty innych krajów lub inne aplikacje.

© 2004 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.