



Rozważania nt. wariantów wdrożenia sieci IPSec VPN i SSL VPN¹

Zawartość dokumentu

1. Wprowadzenie.
2. Sieci IPSec VPN.
3. Sieci SSL VPN.
4. IPSec VPN czy SSL VPN ?
5. Scenariusze zdalnego dostępu.

Wprowadzenie

W ciągu ostatnich kilku lat, w wyniku geograficznego rozproszenia firm i zwiększonej mobilności pracowników, wzrosła dramatycznie tendencja wykorzystania Internetu oraz technik szyfrowania do zdalnego dostępu. Pojawiły się dwa rozwiązania zdalnego dostępu poprzez Internet – wirtualna sieć prywatna zgodna ze standardem zabezpieczeń protokołów internetowych (IPSec VPN) oraz wirtualna sieć prywatna wykorzystująca protokół SSL (SSL VPN). Wybór konkretnej sieci VPN zależy od specyficznych wymagań firmy, w wielu z nich implementuje się oba rozwiązania, ponieważ niektóre wdrożenia dostępu do sieci poprzez SSL uzupełniają się ze standardem IPSec.

Zdalny dostęp, z natury rzeczy, powinien umożliwiać połączenia z odległych węzłów. Ogólnie rzecz biorąc, wspomniane węzły to komputery użytkowników, głównie laptopy lub maszyny stacjonarne, lecz również urządzenia PDA, przypadkowe komputery w kawiarenkach internetowych i inny sprzęt. W przyszłości również telefony komórkowe, czy urządzenia budowane pod konkretne rozwiązania (np. komputery podręczne, które ewidencjonują wypożyczone samochody) będą prawdopodobnie wykorzystywane jako węzły dostępu. Wzrastająca różnorodność urządzeń dostępowych jest głównym czynnikiem wpływającym na szybki rozwój nowych technologii zdalnego dostępu.

Z definicji większość zdalnych użytkowników to osoby posiadające dostęp do wewnętrznych zasobów firmy z węzłów znajdujących się poza granicą bezpieczeństwa danej firmy. Węzły te to potencjalne cele włamywaczy, szukających furtek (ang. backdoor) do zasobów firmy (klient posiadający zdalny dostęp skutecznie zmienia się wówczas w ruter otwierający drogę do firmy). Dlatego też firmy wdrażają zabezpieczenia również na zdalnych węzłach dostępowych. Zabezpieczenia te to: sprawdzanie konfiguracji węzłów, kontrola obecności zapory (firewall) i oprogramowania antywirusowego, ale również wykrywanie oprogramowania szpiegującego (ang. spyware). W zależności od poziomu zaufania zdalnego węzła, posiada on pełny, ograniczony lub zabroniony dostęp do zasobów.

Bezpieczeństwo węzłów zdalnych związane jest z kontrolą dostępu oraz z mechanizmami bezpieczeństwa oferowanymi przez bramę VPN/firewall. Techniki szyfrowania zapewniają skuteczną poufność oraz integralność danych, jednak nie umożliwiają nadawania praw dostępu. Samo prawo ustanowienia przez użytkownika tunelu VPN (wykorzystując IPSec lub SSL) nie powinno umożliwiać mu uzyskania dostępu do wszystkich zasobów. Rozwiązania bezpiecznego zdalnego dostępu powinny dawać administratorom możliwość ograniczenia dostępu zdalnym użytkownikom jedynie do wymaganych zasobów. Ponadto jeżeli dostęp zdalny zapewniany jest

¹ Na podstawie publikacji „IPSec and SSL VPN Deployment Considerations”, P/N 501337, firmy Check Point Software Technologies – wszelkie prawa zastrzeżone.

bardziej zróżnicowanej grupie węzłów, sieć proaktywna (ang. pro-active network) wraz z mechanizmami ochrony przed atakami na poziomie aplikacji minimalizują ryzyko naruszenia bezpieczeństwa wewnętrznych serwerów z potencjalnie niezabezpieczonych węzłów.

Dokument ten przedstawia podstawowe informacje, istotne założenia dla każdej technologii oraz scenariusze wdrożenia, które umożliwią wybranie rozwiązania najbardziej odpowiedniego do potrzeb danej firmy.

Podstawy techniczne

Dwie popularne techniki umożliwiające zdalny dostęp to wirtualna sieć prywatna zgodna ze standardem zabezpieczeń protokołów internetowych (IPSec VPN) oraz wirtualna sieć prywatna wykorzystująca protokół SSL (SSL VPN) zwana również siecią VPN „bez klienta” (ang. „clientless” VPN).

Sieć IPSec VPN

Typowe wdrożenie rozwiązania IPSec (IP Security) VPN składa się z jednej lub większej ilości bram VPN, stanowiących punkty terminujące kryptograficzne kanały dostępu do serwerów zlokalizowanych w sieciach wewnętrznych, oraz z oprogramowania klienta, które musi być zainstalowane na każdym komputerze stanowiącym zdalny punkt dostępowy. Zależnie od przyjętego rozwiązania, klient VPN jest konfigurowany manualnie lub automatycznie. Konfiguracja klienta umożliwia określenie, które pakiety powinny zostać zaszyfrowane oraz którą bramę wykorzystać do zestawienia tunelu VPN. W przypadku wirtualnych sieci prywatnych typu „site-to-site” możliwa jest współpraca rozwiązań pochodzących od różnych dostawców. Standard IPSec zastosowano również w sieciach ze zdalnym dostępem typu „client-site”. W tym przypadku jednak współdziałanie pomiędzy rozwiązaniami poszczególnych dostawców nie jest już tak ujednolicone, gdyż stworzono wiele rozszerzeń standardu IPSec, w celu wsparcia zdalnego dostępu realizowanego w różnych konfiguracjach (np. w sieciach z translacją adresów IP - NAT traversal).

IPSec jest dojrzałym standardem, wdrażanym na całym świecie przez wielu dostawców, oferujących swoje rozwiązania jako bramy VPN, serwery oraz oprogramowanie klienckie. Standard IPSec obsługuje mechanizmy silnego szyfrowania oraz zapewniania integralności danych. Jest to technologia VPN funkcjonująca w warstwie sieciowej, co oznacza, że działa niezależnie od aplikacji, która ją wykorzystuje. IPSec hermetyzuje oryginalny pakiet IP za pomocą własnego pakietu, ukrywając w ten sposób wszelkie informacje protokołu aplikacji. Zestawiony tunel IPSec umożliwia obsługę dowolnej ilości połączeń różnego rodzaju (WWW, poczta, transfer plików, VoIP), z których każde przeznaczone jest do innego serwera, znajdującego się za bramą VPN.

Zalety/wady rozwiązania IPSec VPN

Zalety:

- obsługa wszystkich usług i typów IP tj. ICMP, VoIP, SQL*Net, Citrix ICA,
- to samo rozwiązanie funkcjonuje w przypadku wdrożeń client-to-site, site-to-site oraz client-to-client,
- klient IPSec zapewnia możliwość wbudowania innych funkcji bezpieczeństwa, np. osobistych zapór (firewall), weryfikacji konfiguracji i in.,
- bramy VPN zintegrowane są standardowo z zaporami sieciowymi realizującymi funkcje kontroli dostępu, filtrowania treści, ochrony przed atakami oraz innymi zabezpieczeniami.

Wady:

- wymaga instalacji oprogramowania na stacji klienta; nie zawsze obsługiwane są wszystkie systemy operacyjne,
- zapory sieciowe i inne urządzenia pomiędzy klientem i bramą VPN mogą niekorzystnie wpływać na możliwość zestawiania połączeń VPN,

- współdziałanie pomiędzy klientem IPSec jednego dostawcy a serwerem/bramą IPSec innego jest zazwyczaj utrudnione.

Sieć SSL VPN

SSL jest bezpiecznym protokołem transportowym, powszechnie wykorzystywanym do zapewnienia poufności i bezpieczeństwa transakcji np. w bankowości czy handlu elektronicznym (łącza z HTTPS jak np. <https://www.example.com>). Często sieci SSL VPN nazywane są sieciami „bez klienta” (ang. clientless), ponieważ większość przeglądarek internetowych obsługuje protokół SSL i właśnie one są wykorzystywane jako oprogramowanie klienta. Jest to przeciwieństwo rozwiązania opartego o IPSec, gdzie na każdym komputerze wykorzystującym zdalny dostęp musi być zainstalowane oprogramowanie klienckie dostarczone przez producenta. Rozwiązanie SSL VPN standardowo oznacza zdalny dostęp do sieci poprzez bramę SSL VPN, lecz może również zawierać aplikacje obsługujące SSL np. klienty poczty (Ms Outlook, Eudora).

SSL to protokół, który działa poprzez TCP. Podobnie jak w IPSec istnieje tutaj faza wstępna, przed nawiązaniem połączenia, w której negocjowanych i weryfikowanych jest kilka parametrów:

- uwierzytelnienie serwera przez klienta za pomocą certyfikatów cyfrowych,
- opcjonalne uwierzytelnienie klienta przez serwer za pomocą certyfikatów cyfrowych (lub innych metod),
- bezpieczne wygenerowanie kluczy sesji, wykorzystywanych do szyfrowania i sprawdzania integralności danych.

SSL wykorzystuje różne algorytmy generowania kluczy publicznych (RSA, DSA), symetrycznych (DES, 3DES, RC4) oraz algorytmy integralności danych (MD5, SHA-1).

Istnieją dwa sposoby wdrożenia zdalnego dostępu z wykorzystaniem protokołu SSL. W pierwszym przypadku poszczególne serwery wykorzystując oprogramowanie SSL samodzielnie terminują tunele zestawiane przez zdalnych użytkowników. Alternatywą dla takiego rozwiązania jest brama VPN, która z jednej strony stanowi interfejs terminujący tunele VPN zdalnych użytkowników, komunikując się jednocześnie z wewnętrznym serwerem w jego rodzimym formacie.

Wtyczki SSL VPN w przeglądarkach WWW

Ostatnio w sieciach SSL VPN pojawiły się rozwiązania umożliwiające zdalnemu węzłowi tunelowanie ruchu pochodzącego z aplikacji klient/serwer za pomocą wtyczki (ang. plug-in) przeglądarki internetowej, zamiast instalowanego oprogramowania do zdalnego dostępu. Użytkownicy uwierzytelniają się w portalu WWW (standardowo jest to brama sieci SSL VPN) oraz pobierają niewielką wtyczkę (formant ActiveX lub agent Java). Następnie, w sposób niewidoczny dla użytkownika, przechwytyują one cały ruch pomiędzy klientem a serwerem i tunelują go poprzez protokół SSL. Rozszerzenia różnią się zakresem obsługiwanych aplikacji. Niektóre obsługują tylko ruch TCP, a wiele z nich nie wspomaga dynamicznych aplikacji np. FTP czy VoIP.

Zalety:

- protokół SSL jest zintegrowany ze wszystkimi czołowymi przeglądarkami (Internet Explorer, Netscape, Mozilla),
- popularne aplikacje np. klienty i serwery pocztowe obsługują protokół SSL.
- działa niewidocznie dla NAT, serwerów proxy oraz większości zapór, które pozwalają na ruch SSL.
- rozszerzenia przeglądarki internetowej umożliwiają aplikacjom klient-serwer łączność na poziomie sieci poprzez protokół SSL.

Wady:

- obsługuje jedynie macierzyste usługi TCP: web (HTTP) lub pocztę elektroniczną (POP3/IMAP/SMTP),
- SSL w przeciwieństwie do IPSec wymaga od bramy użycia większej ilości zasobów,

- w przypadku rozwiązania typu „bez klienta” (ang. clientless), klient nie posiada zainstalowanego żadnego oprogramowania firmowego, co daje ograniczoną możliwość umieszczenia na zdalnym węźle oprogramowania zabezpieczającego (zapory, sprawdzenia integralności),
- jeżeli sesje nie są terminowane na poziomie zapory sieciowej (ang. firewall), wymagane jest tworzenie dziur w firmowych zaporach poprzez które przechodzi tunel, co uniemożliwia im inspekcje danych w połączeniach HTTPS,
- rozszerzenia przeglądarek internetowych mogą obsługiwać ograniczoną liczbę aplikacji lub wymagać (do prawidłowego działania) uprawnień administracyjnych na danej maszynie,
- nie wykorzystywane w sieciach VPN typu site-to-site VPN; standardowo używany jest tutaj IPSec co powoduje, że w przypadku sieci ze zdalnym dostępem oraz sieci, które takiego dostępu nie posiadają zastosowane muszą być dwie odrębne technologie.

Zdalny dostęp przez IPSec VPN czy SSL VPN ?

Wybór tej czy innej technologii zależy od wymagań i celów stawianych w projekcie zdalnego dostępu. Jeżeli wybrano już technologię, następnym krokiem jest znalezienie rozwiązania, które najlepiej spełnia określone wymagania. Wybierając jedno z oferowanych przez dostawców rozwiązanie, które opiera się na wybranej technologii, bierze się pod uwagę wydajność, łatwość zarządzania, koszt wdrożenia, łatwość integracji z istniejącymi rozwiązaniami, wsparcie ze strony dostawcy i inne tego typu kryteria.

	IPSec VPN	SSL VPN
Dostępność aplikacji	Wszystkie aplikacje IP (aplikacje WWW, firmowe, poczta elektroniczna, VoIP oraz multimedia).	Głównie aplikacje WWW.
Wymagane oprogramowanie	Oprogramowanie klienckie IPSec.	Standardowa przeglądarka internetowa.
Udostępnianie informacji	Dostęp posiadają tylko wyznaczone osoby/komputery.	Dostęp z dowolnego miejsca np. kawiarni internetowych. Informacje mogą być pozostawione (celowo lub niechcący).
Poziom bezpieczeństwa klienta	Średni – Wysoki (zależnie od oprogramowania zainstalowanego na stacji klienta).	Niski – Średni (średni wymaga dedykowanego oprogramowania na stacji klienta).
Skalowalność	Rozwiązanie wysoce skalowalne (potwierdzone dziesiątkami tysięcy wdrożeń u klienta).	Rozwiązanie wysoce skalowalne i łatwe do wdrożenia.
Metody uwierzytelniania	Obsługuje wiele metod uwierzytelniania. W przypadku niektórych dostawców wbudowana infrastruktura klucza publicznego (PKI).	Obsługuje wiele metod uwierzytelniania. Wykorzystanie opcji silnego uwierzytelniania wymaga dodatkowych nakładów finansowych i ogranicza zbiór urządzeń dostępu.
Konsekwencje wdrożonych zabezpieczeń	Poszerza infrastrukturę bezpieczeństwa o zdalny dostęp. Zwiększa bezpieczeństwo węzłów poprzez zintegrowane rozwiązania np. osobistą bramę (firewall).	Ograniczony nadzór nad dostępem do informacji i środowiskiem klientów. Dobre rozwiązanie przy dostępie do mniej wrażliwych informacji.
Idealne rozwiązanie dla:	bezpiecznego dostępu dla pracowników oraz pomiędzy ośrodkami.	dostępu zewnętrznym klientom poprzez przeglądarkę WWW.

Analizując powyższe wady i zalety obu rozwiązań można dojść do następujących ogólnych wniosków:

- IPSec jest lepszym rozwiązaniem kiedy w projekcie uwzględniono przynajmniej jedno z poniższych wymagań:

- ✓ Firma potrzebuje ogólnej infrastruktury do obsługi szerokiego zakresu protokołów sieciowych, a nie wyłącznie dostępu do sieci WWW oraz poczty elektronicznej.
 - ✓ Organizacja jest w stanie administrować komputerem, posiadającym zdalny dostęp do zasobów.
 - ✓ Wymagane są zabezpieczenia (np. osobista zapora) komputera, posiadającego zdalny dostęp. Na przykład administrator może zabronić dostępu użytkownikom korzystającym z komputerów w kawiarenkach internetowych, ze względu na nieznaną stan zabezpieczeń tych maszyn.
- SSL jest najlepiej pasującym rozwiązaniem, jeżeli w projekcie uwzględniono przynajmniej jedno z poniższych wymagań:
 - ✓ Zdalni użytkownicy wykorzystują dostęp jedynie w celu korzystania z aplikacji WWW i poczty elektronicznej.
 - ✓ Wymagany jest dostęp do zasobów z dowolnego urządzenia (np. laptopów, komputerów domowych, kawiarni internetowych itp.).
 - ✓ Firmowa zapora lub dostawca usług internetowych (ISP) nie zezwala na połączenia IPSec (np. blokując negocjowanie IKE), bez blokowania protokołu SSL.
 - ✓ Firmy nie mają kontroli nad konfiguracją komputera posiadającego zdalny dostęp do zasobów.
 - ✓ Nie jest możliwa instalacja oprogramowania zapewniającego zdalny dostęp na komputerze użytkownika.

Scenariusze zdalnego dostępu

Mimo, że każda firma posiada swój własny niepowtarzalny zestaw wymagań odnośnie zdalnego dostępu, istnieje kilka kategorii zdalnych użytkowników, które wykorzystuje się wybierając wdrożenie któregoś z rozwiązań (IPSec lub SSL).

Poniższe scenariusze można potraktować jako pomoc przy wybieraniu odpowiedniej technologii dla firmy. Poczyniono tutaj dwa uogólnienia. Po pierwsze, im większa jest różnorodność węzłów (od zarządzanego komputera pracownika firmy do maszyn w kawiarence internetowej), tym bardziej preferowany scenariusz przechodzi od rozwiązania IPSec do SSL. Po drugie, jeżeli scenariusz zmienia się od wykorzystania aplikacji w architekturze klient-serwer do używania wyłącznie aplikacji WWW, preferowane rozwiązanie również przechodzi od IPSec do SSL.

Warto zauważyć fakt, że w wielu scenariuszach najlepszym rozwiązaniem okazuje się wdrożenie zarówno SSL, jak i IPSec.

Zdalni administratorzy (ang. heavy remote users)

Zaliczani są tutaj administratorzy systemu, jak i inżynierowie. Ten rodzaj użytkowników wykorzystuje standardowo rozwiązanie IPSec, istnieją bowiem dwa poważne czynniki, które tego wymagają. Po pierwsze, użytkownicy w swojej pracy wykorzystują głównie specyficzne aplikacje (nie WWW). Po drugie, środowiska systemowe użytkowników są zazwyczaj administrowane przez firmę.

Zdalni użytkownicy (ang. light remote users)

Przykładem są tutaj użytkownicy pracujący na własnych maszynach poza firmą (ang. Day Extenders). Najlepszym rozwiązaniem dla tego rodzaju użytkowników jest SSL VPN. Domowy komputer to środowisko częściowo zarządzane i niedostępne publicznie dla każdego. Maszyna ta, zarządzana przez użytkownika, a nie firmę, może mieć lub nie mieć zainstalowane oprogramowanie zabezpieczające, np. zapory czy programy antywirusowe. Firma sama decyduje na jaki dostęp pozwolić tego typu użytkownikom. Na przykład, zezwala na większy poziom dostępu, jeżeli żądanie dotarło z komputera posiadającego zainstalowaną zaporę (firewall), a ogranicza dostęp dla maszyn bez takiego oprogramowania. Ponieważ dostawcy rozwiązań SSL VPN stosują różne miary zabezpieczeń, decyzja o wyborze dostępu VPN jest podejmowana na podstawie oceny bezpieczeństwa zapewnianego przez poszczególne rozwiązania.

Pracownicy mobilni (ang. mobile employees)

Przykładem są tutaj sprzedawcy czy kierownicy. W tym przypadku wybrać można IPSec, SSL lub oba rozwiązania. Dla pracowników mobilnych, korzystających z firmowego laptopa, IPSec będzie idealnym rozwiązaniem, ponieważ środowiskiem takim można zarządzać, a wiele klientów IPSec posiada oprogramowanie zabezpieczające np. osobiste zapory. Jednak w niektórych przypadkach dodatkowo wykorzystuje się rozwiązanie SSL. Na przykład, wielu pracowników mobilnych wykorzystuje do kontaktu z firmą publicznie dostępne komputery (w hotelu, kawiarence internetowej). Środowiska te nie są zarządzane przez firmę, dlatego idealnie pasuje tutaj rozwiązanie SSL do obsługi poczty elektronicznej i dostępu do zasobów poprzez WWW. Korzystanie w tym przypadku z aplikacji klient-serwer nie jest możliwe, gdyż oprogramowanie klienta nie może być zainstalowane na zdalnej maszynie.

Pracownicy zdalni (ang. on-site workers)

Zaliczani są tutaj np. konsultanci oraz osoby pracujące na zlecenie. W tym przypadku lepszym rozwiązaniem okazuje się sieć SSL VPN. Tego typu pracownicy, pracując na swoich własnych komputerach, potrzebują dostępu do wewnętrznej sieci. Rozwiązanie SSL VPN umożliwia bezpieczny dostęp do zasobów firmy bez potrzeby instalowania jakiegokolwiek oprogramowania na komputerach pracowniczych.

Partnerzy z dostępem do ekstranetu (ang. extranet partners)

Przykładem są tutaj partnerzy korzystający z portalu WWW w celu wymiany informacji lub dostępu do aplikacji WWW. Ten rodzaj dostępu jest najbardziej typowym dla rozwiązania SSL VPN, ponieważ partner posiada dostęp z komputera, który nie jest kontrolowany przez firmę. Produkty implementujące SSL VPN powszechnie udostępniają użytkownikowi portal WWW, który zapewnia wygodne miejsce do gromadzenia danych dla partnerów. Rozwiązanie to posiada również dodatkową korzyść. Mianowicie nie ma potrzeby tworzenia oddzielnej sieci dla zasobów ekstranetu. Jednak dla organizacji, wymagających dostępu do aplikacji klient-serwer, lepszym rozwiązaniem jest IPSec, gdyż w środowisku, gdzie koniecznym jest zainstalowanie „użytkowej” aplikacji klienckiej, dodatkowa instalacja klienta VPN jest mniejszym problemem.

Rozwiązania IPSec i SSL firmy Check Point

IPSec VPN	IPSec VPN i SSL VPN	SSL VPN
VPN-1 z SecureRemote lub SecureClient	VPN-1 z SSL Network Extender	Connectra Web Security Gateway (zawiera SSL Network Extender)

VPN-1

Firma [Check Point](#) oferuje najbardziej wszechstronny zbiór produktów i technologii umożliwiających zdalny dostęp oraz tworzenie intranetowych i ekstranetowych sieci VPN. Bramy zabezpieczające VPN-1[®]/FireWall-1[®] chronią prywatność połączeń biznesowych przez Internet, zabezpieczając jednocześnie istotne zasoby sieci przed nieuprawnionym dostępem. Zależnie od wielkości i złożoności sieci do wyboru jest kilka produktów:

- VPN-1 Pro™ – najbardziej wszechstronne zabezpieczenie dla dużych, złożonych sieci.
- VPN-1 Express – bezproblemowe zabezpieczenie firm, które zatrudniają do 500 pracowników i posiadają wiele ośrodków (ang. sites).
- VPN-1 Edge™ – bezpieczna łączność z odległymi ośrodkami i sieciami VPN dużej skali.

Poniżej przedstawiono rozwiązania IPSec i SSL dostępne dla VPN-1:

- VPN-1 SecureRemote™ – udostępnia podstawowe możliwości IPSec, m.in. silne i elastyczne uwierzytelnianie oraz prostą konfigurację po stronie klienta.

- VPN-1 SecureClient™ – jest nadzbiorem (ang. superset) VPN-1 SecuRemote, udostępniającym zaawansowane technologie zdalnego dostępu (w tym osobistą zaporę z centralnie zarządzaną polityką, gwarancję zabezpieczenia klienta, kompresję IP, automatyczną wewnętrzną aktualizację oprogramowania oraz tryb OfficeMode, który przypisuje zdalnemu klientowi wirtualny adres IP, co eliminuje wszystkie znane kwestie związane z translacją NAT). Oferowana hermetyzacja UDP również jest w tym przypadku pomocna. Wszystkie te elementy sprawiają, że użytkownik ma wrażenie, jakby znajdował się w wewnętrznej sieci LAN.
- SSL Network Extender™ – zapewnia bezpieczny dostęp przez Internet. Umożliwia zdalnym użytkownikom podłączanie aplikacji klient-serwer do VPN-1 za pomocą przeglądarki WWW.

Connectra

Connectra™ firmy Check Point jest kompletną bramą zabezpieczającą, która zapewnia zarówno SSL VPN jak i zintegrowane zabezpieczenie WWW w postaci pojedynczego, ujednoczonego rozwiązania. Połączenie funkcji zapewniania połączeń zdalnych i bezpieczeństwa w jednej platformie pozwala na wdrożenie w firmie rozwiązania SSL VPN w sposób bezpieczny i bezproblemowy. Zintegrowanie SSL VPN z innymi produktami firmy Check Point (Application Intelligence™, Web Intelligence™ i architekturą SMART (ang. Security Management Architecture)) zapewnia niewiarygodnie bezpieczną łączność opartą o WWW.

SSL Network Extender

SSL Network Extender firmy Check Point zapewnia bezpieczny dostęp przez Internet dla partnerów biznesowych i pracowników, którzy potrzebują zdalnego dostępu do wewnętrznych aplikacji firmy. Dostępny jako rozszerzenie dla kilku produktów firmy Check Point, umożliwia zdalnym użytkownikom korzystanie z aplikacji klient-serwer za pomocą przeglądarki internetowej. Posiada również najbardziej rozbudowany zbiór funkcji oraz wspólną infrastrukturę zarządzającą wśród rozwiązań dostępnych obecnie na rynku. SSL Network Extender jest częścią produktu Connectra i opcjonalnie modułem dodatkowym dla VPN-1.

Firma Check Point Software Technologies

Firma Check Point Software Technologies jest światowym liderem rozwiązań przeznaczonych do zabezpieczania Internetu, jak również liderem rynku sieci VPN i zapór (firewalls). Bazując na INSPECT (najbardziej adaptacyjnej i inteligentnej technologii inspekcji) oraz na administrowaniu SMART (które zapewnia najniższy poziom TCO dla zarządzania infrastrukturą bezpieczeństwa) rozwiązania firmy Check Point są najbardziej wiarygodnymi i szeroko stosowanymi rozwiązaniami na całym świecie. Są one sprzedawane, integrowane i serwisowane przez sieć 1900 certyfikowanych partnerów w 86 krajach. W celu uzyskania większej ilości informacji należy zadzwonić pod numer (800) 429-4391 lub (650) 628-2000 lub odwiedzić stronę <http://www.checkpoint.com> lub <http://www.opsec.com>.