WIRTUALNE SIECI PRYWATNE I BEZPIECZNY ZDALNY DOSTĘP

WPROWADZENIE.

Powstanie Internetu stworzyło nowy rozdział w ludzkiej cywilizacji. Ludzie nie są już przywiązani do wolno aktualizowanych źródeł informacji, takich jak biblioteki. Gwałtowny wzrost liczby osób poszukujących różnorodnych treści również pobudził chęć mobilności. Jeśli ktoś może szukać informacji przebywając w połowie drogi dookoła świata z domu, dlaczego nie mieć tego samego w lokalnej kawiarni lub podczas podróży służbowej? Ta rewolucja informacyjna dała możliwość dostarczania informacji i usług konsumentom, firmom i pracownikom w praktycznie dowolnym miejscu na świecie i na wielu platformach mobilnych. Czasy koncentrowania się na ochronie na obrzeżach sieci minęły i minęły więcej czasu, niż ludzie mogą sobie wyobrazić. Laptopy przewodzą początkowej sile mobilnej. Chociaż dostęp do pełnej mocy obliczeniowej laptopa jest przydatny w niektórych przypadkach, nawet lekkie wersje są nieporęczne w podróży i mają stosunkowo krótką żywotność baterii. Smartfony i tablety mieszczące się w dłoni, kieszeni lub torebce zapewniają teraz dostęp do częściej używanych aplikacji

Rozpuszczanie granic.

Powszechny dostęp do Internetu na nowo zdefiniował dynamikę ochrony sieci i granic. Wcześniej firmy koncentrowały się na ochronie sieci wewnętrznej i systemów wystawionych na działanie Internetu. Zapora na obwodzie wystarczyła, aby powstrzymać cyfrowe drapieżniki. Większym wyzwaniem jest teraz utrzymanie bezpieczeństwa sieci wewnętrznej, gdy pracownicy korzystają z technologii mobilnych w domu lub podczas podróży. Kolejną komplikacją problemu jest to, jak umożliwić innym partnerom biznesowym - ale nie intruzom - bezpieczny dostęp do systemów i informacji, za których ochronę jesteś odpowiedzialny. Organizacje duże i małe nie mogą oczekiwać utrzymania przewagi konkurencyjnej poprzez ograniczenie sieci pracowników i dostępu do informacji w granicach miejsca pracy. Podróżujący pracownicy mogą teraz utrzymywać bezpośrednią komunikację z osobami w biurze. Pracownicy, którzy utknęli w domu z powodu złej pogody lub choroby, mogą nadal funkcjonować, mając bezpośredni dostęp do niezbędnych informacji. Ta mobilność zapewnia organizacjom realną metodę utrzymania zróżnicowanej geograficznie siły roboczej, która umożliwia ludziom pracę w bliższej odległości od klientów i partnerów. Organizacje wdrażają również elastyczne rozwiązania mobilne, które mogą działać na smartfonach i tabletach. Zamiast przynosić firmowy laptop na wizytę u klienta, sprzedawca może używać tabletu do prezentowania informacji o produkcie, wprowadzania / zmiany informacji o zamówieniu i uzyskiwania dostępu do innych zasobów wewnętrznych. Istnieje również znaczny ruch umożliwiający pracownikom korzystanie z osobistego laptopa lub urządzenia inteligentnego w celu uzyskania dostępu do zasobów wewnętrznych - i dowody na to, że taka polityka może faktycznie zwiększyć koszty technologii informacyjnej zamiast je zmniejszać. Tendencja ta zwiększa potencjalny profil ryzyka, ponieważ organizacja musi zapewnić bezpieczeństwo na różnych warstwach przy niewielkiej lub żadnej kontroli nad zabezpieczeniami urządzeń osobistych, które mogą łączyć się z zasobami wewnętrznymi. Bring Your Own Device (BYOD) ma coraz większe znaczenie w dyskusjach na temat produktywności i bezpieczeństwa. Wraz ze wzrostem sieci dostawców, dostawców i partnerów organizacji rośnie konieczność udostępniania informacji. Organizacja musi szukać metod, które umożliwią tym zewnętrznym podmiotom dostęp do odpowiednich informacji bez ujawniania nieistotnych informacji. Udostępnianie informacji nie ogranicza zaangażowania partnerów. Mogą zaistnieć sytuacje, w których personel wewnętrzny nie ma niezbędnego doświadczenia, aby opracować lub wspierać określone systemy informacyjne. Chociaż zatrudnienie konsultanta na stanowisku pracownika lub dyżurnego może być zbyt kosztowne, organizacja może zdecydować się na zezwolenie dostawcy na zdalny dostęp do określonych części sieci wewnętrznej w celu zapewnienia niezbędnego poziomu usług. Te części sieci nazywane są ekstranetami. Klienci nadal domagają się coraz

większej wygody. Sektor bankowy jest użytecznym przykładem tego, jak rosną wymagania konsumentów i jak biznes reaguje na te potrzeby. Zamiast iść do lokalnego banku, możliwość prowadzenia pewnych zapytań i transakcji było możliwe przez telefon. Ograniczenia tej technologii wymagały jeszcze większych możliwości, jakim był dostęp do rachunków i innych usług bankowych przez Internet. Teraz konsument ma wizualny interfejs typu „wskaż i kliknij / dotknij" zamiast skomputeryzowanego głosowego i numerycznego menu. Te same wymogi dotyczące wygody występują w przypadku sprzedaży towarów i usług. Konsumenci mogą nie chcieć chodzić do tradycyjnego sklepu, aby dokonać zakupów, ale dzięki obecności w Internecie organizacja może sprostać temu zapotrzebowaniu, udostępniając witrynę e-commerce, która daje konsumentowi możliwość przeglądania i kupowania produktów pod adresem czas i miejsce wyboru konsumenta.

Bezpieczny dostęp zdalny.

Chociaż konsekwencje niespełnienia wymagań partnerów i / lub konsumentów są oczywiste, organizacje przeprowadzają wiele planowania i przeglądów, aby zapewnić, że spełnienie tych wymagań nie zagraża bezpieczeństwu systemów informatycznych, które napędzają biznes. Dwie podstawowe technologie zapewniające bezpieczny dostęp zdalny to wirtualna sieć prywatna (VPN) i ekstranet. Sieć VPN to sieć wirtualna nakładająca się na istniejący zestaw sieci fizycznych i logicznych. Typowa implementacja VPN to bezpieczne połączenie, które umożliwia zdalnemu klientowi dostęp do wewnętrznej sieci organizacji przez zaszyfrowany tunel. VPN mają również możliwość rozszerzenia wszystkich lub tylko wybranych fragmentów sieci do innych lokalizacji w organizacji. Extranet spełnia niektóre z tych samych celów, co VPN, z naciskiem na udostępnianie informacji i handel elektroniczny. Zamiast łączyć się z siecią wewnętrzną, klient ustanawia szyfrowane połączenie z serwerem aplikacji WWW znajdującym się w zewnętrznej strefie usług. Ekstranety mogą wprowadzić dodatkową złożoność, ponieważ systemy skierowane na zewnątrz zwykle wymagają dostępu do jednego lub większej liczby zasobów informacyjnych w sieci wewnętrznej.

VPN

Istota VPN jest prosta: utwórz zaszyfrowany tunel do sieci wewnętrznej, aby chronić przesyłane dane. Jednak koncepcje leżące u podstaw technologii VPN są złożone i wymagają długiego planowania, aby zapewnić najlepszą możliwą implementację. Sieci VPN zwykle dzielą się na dwie kategorie: sieci VPN z dostępem zdalnym i sieci VPN typu site-to-site. Każdy typ sieci VPN ma wiele dróg implementacji, a każda z nich ma inne wymagania. Umożliwienie ludziom zdalnego dostępu do zasobów sieci wewnętrznej ma istotne konsekwencje dla zapewnienia bezpieczeństwa informacji. Główne cele sieci VPN w zakresie zapewniania informacji to bezpieczne rozszerzenie sieci wewnętrznej, ochrona danych podczas transmisji i minimalizacja wpływu tego procesu na bezpieczeństwo. Smartfony i tablety często mają również możliwość ustanowienia tunelu VPN. Bez względu na rodzaj urządzenia mobilnego organizacja musi spełniać wymagania zdalnego dostępu przy jak najmniejszym dodatkowym ryzyku. Właściwie zaprojektowana, zarządzana, monitorowana i zabezpieczona sieć wewnętrzna może zapewnić względnie bezpieczne środowisko do udostępniania danych. Jednak internet jest wrogim środowiskiem. Urządzenie mobilne nie może już liczyć na zabezpieczenia sieci wewnętrznej jako cyfrowej strefy komfortu. Internetowe hotspoty do publicznego dostępu, takie jak te w restauracjach, na lotniskach i w hotelach, stwarzają jeszcze większe wyzwania dla zapewnienia informacji. Te publiczne lokalizacje (wiele z nich skonfigurowanych pod kątem otwartego dostępu) tworzą witryny dla złośliwych aktorów, które przechwytują ruch sieciowy w celu zebrania informacji, takich jak poświadczenia, informacje finansowe i dane intelektualne. Prawidłowo wdrożone i zarządzane sieci VPN i ekstranety mają możliwość udaremnienia tego typu monitorowania poprzez wysyłanie danych za pośrednictwem zaszyfrowanych kanałów. Ponieważ potrzeba zaostrzenia bardziej rygorystycznych środków bezpieczeństwa utrzymuje się, rośnie też potencjalne zagrożenie dla użytkownika

końcowego. Użytkownik szybko zorientuje się, że wyłączenie lokalnych środków bezpieczeństwa może przynieść korzyści. Bez uruchomionej zapory klienta szybkość połączenia może wzrosnąć. Co gorsza, wyłączając zabezpieczenia, użytkownik może być w stanie zainstalować i uruchomić oprogramowanie, które w innym przypadku zostało zablokowane. Celem menedżerów bezpieczeństwa musi być utrzymanie wysokiego poziomu bezpieczeństwa, który jest niewidoczny dla użytkownika. Proces ustanawiania tunelu VPN lub uzyskiwania dostępu do zasobów wewnętrznych powinien wydawać się autoryzowanemu użytkownikowi łatwy, a działająca w tle infrastruktura bezpieczeństwa zapewnia niezbędny poziom ochrony bez zakłócania produktywności legalnych użytkowników. W tym rozdziale przedstawiono podstawy do zrozumienia różnych typów, terminologii i zastosowań sieci VPN i ekstranetów.

VPN DO ZDALNEGO DOSTĘPU.

Najpopularniejszym zastosowaniem VPN jest bezpieczny, zdalny dostęp klienta. Pozwala to autoryzowanemu użytkownikowi połączyć się z VPN i uzyskać dostęp do zasobów wewnętrznych z dowolnego miejsca z połączeniem internetowym, przy jednoczesnym zachowaniu bezpieczeństwa transmisji. Sieci VPN dostępu zdalnego toczą nieustającą walkę między tradycyjnymi protokołami internetowymi (IPsec) a coraz bardziej popularnymi i potężnymi sieciami VPN z zabezpieczeniami na poziomie transportu / Secure Sockets Layer (TLS / SSL). Każdy typ sieci VPN ma różne zalety i każdy gwarantuje dokładne zbadanie przed wyborem technologii, która najlepiej odpowiada potrzebom organizacyjnym.

IPsec.

IPsec to zestaw protokołów warstwy sieciowej przeznaczony do konfigurowania i ochrony transmisji VPN. Tradycyjne implementacje IPsec VPN wykorzystują aplikację kliencką lub wbudowaną usługę systemu operacyjnego do ustanowienia tunelu VPN do sieci wewnętrznej.

Wymiana kluczy i zarządzanie nimi.

Jednym z najbardziej złożonych aspektów protokołu IPsec jest wymiana kluczy i zarządzanie nimi. IPsec wykorzystuje Internet Key Exchange (IKE) w celu ułatwienia tworzenia i zarządzania Security Association (SA). Kluczowe punkty IKE Fazy 1 i 2 obejmują:

* Faza 1 może używać trybu głównego lub trybu agresywnego, aby utworzyć początkowe powiązanie zabezpieczeń IKE. Najpopularniejszą implementacją jest tryb główny, składający się z trzech par pakietów.

* Pierwsza para negocjuje czteroparametrowy pakiet ochrony:

* Algorytm szyfrowania (np. Advanced Encryption Standard, AES),

* Algorytm ochrony integralności (np. Tryb uwierzytelniania wiadomości hashed [HMAC] z algorytmem Secure Hash, SHA-256),

* Metoda uwierzytelniania (np. Klucz wstępny lub certyfikat PKI) i

* Grupa Diffiego-Hellmana

* Druga para wymienia klucze szyfrowania za pomocą Diffie-Hellman.

* Trzecia para uwierzytelnia każdą stronę połączenia z drugą.

Tryb agresywny realizuje to samo zadanie, używając tylko trzech pakietów:

* Pierwsze dwa komunikaty negocjują parametry IKE SA i dokonują wymiany kluczy.

* Druga i trzecia wiadomość uwierzytelniają między sobą punkty końcowe.

* Internet Key Exchange Version 2 (IKEv2), zdefiniowany w RFC 5282,8, jest zaktualizowaną wersją, chociaż nie jest kompatybilna z wersją 1. Ta nowa wersja próbuje naprawić niektóre niedociągnięcia pierwotnej implementacji IKE.

* Niektóre ulepszenia IKE w wersji 2 obejmują:

* Znacznie mniej specyfikacji RFC,

* Zmniejszona liczba wymian wiadomości,

* Mniej metod kryptograficznych,

* Wbudowane zabezpieczenia przed odmową usługi (DoS),

* Wykrywanie i zarządzanie stanem, i prawdopodobnie najważniejsze,

* Translacja adresów sieciowych (NAT) 9 przechodzenie przez protokół datagramów użytkownika (UDP). 10

Jeśli organizacja w dużej mierze zależy od protokołu IPsec, jedno lub więcej z tych ulepszeń może sprawić, że IKEv2 będzie niezwykle korzystny i stworzy znacznie bardziej odporną i lepiej funkcjonującą usługę VPN.

* Faza 2 używa trybu szybkiego do ustalenia adresów źródłowych IPsec (SA).

* Każda strona połączenia zachowa IPsec SA w swojej bazie danych SAD (Security Association Database).

* Urządzenie inicjujące tworzy i wysyła propozycję SA do urządzenia VPN.

* Urządzenie VPN odpowie swoim wyborem SA i kolejnym hashem w celu uwierzytelnienia połączenia.

* Urządzenie inicjujące odpowiada następnie hashem, które generuje z poprzedniego żądania.

* Jeśli hash pasuje do wyzwania z urządzenia VPN, SA przechodzi do SAD i połączenie jest kontynuowane.

Nagłówek uwierzytelniania a hermetyzacja ładunku bezpieczeństwa.

IPsec zapewnia dwa protokoły bezpieczeństwa do ochrony hermetyzowanych danych. Nagłówek uwierzytelniania (AH) chroni integralność nagłówka pakietu i ładunku za pomocą szyfrowania kryptograficznego, aby zapewnić, że dane nie ulegną zmianie. Encapsulating Security Payload (ESP) jest bardziej powszechną implementacją, ponieważ nie tylko zapewnia ochronę integralności AH, ale także chroni poufność poprzez szyfrowanie całego oryginalnego pakietu i tworzenie nowego nagłówka IP. AH i ESP mogą przesyłać dane w trybie transportowym lub tunelowym:

* Tryb transportu zachowuje oryginalne informacje nagłówka IP, zapewniając jednocześnie integralność i poufność ładunku.

* Tryb tunelowy zapewnia integralność i ochronę poufności nagłówka IP i ładunku.

Ponieważ tryb transportu używa oryginalnych informacji nagłówka IP, ten tryb stwarza niezgodności z translacją adresów sieciowych (NAT) z powodu sprawdzania integralności czwartej warstwy. NAT

powoduje, że adres IP pakietu zmienia się podczas przesyłania, co z kolei powoduje niepowodzenie sprawdzania integralności. W związku z tym tryb tunelowy jest podstawową metodą połączeń sieci VPN typu host-brama i brama-brama.

Transport Layer Security.

Protokół Transport Layer Security (TLS) zapewnia metodę ochrony komunikacji klient / serwer. Jedną z najbardziej rozpoznawalnych implementacji TLS jest Secure Sockets Layer (SSL), która stanowi podstawę protokołu HTTPS. Chociaż tu są używane zamiennie protokoły TLS i SSL, ponieważ wiele produktów obsługuje oba, istnieją pewne różnice. TLS to kolejna ewolucja protokołu SSL opracowanego przez firmę Netscape, ponieważ jest to protokół o otwartych standardach obsługiwany przez Internet Engineering Task Force (IETF) i zapewnia zwiększone możliwości bezpieczeństwa. Implementacja TLS / SSL jest znacznie mniej skomplikowana (choć niekoniecznie bezpieczniejsza) niż IPsec i zapewnia 256-bitowe możliwości szyfrowania, które już istnieją w praktycznie wszystkich systemach podłączonych do Internetu. Klient udostępnia parametry związane z SSL do negocjowania połączenia HTTPS z serwerem. Następnie serwer odpowiada, podając wynegocjowane parametry związane z protokołem SSL, a także swój certyfikat cyfrowy. Następnie klient używa certyfikatu do uwierzytelnienia serwera. Jeśli uwierzytelnienie powiedzie się, klient i serwer ustalają klucze szyfrowania używane do ochrony sesji i rozpoczynają szyfrowaną komunikację. Chociaż muszą zaistnieć bardzo specyficzne warunki, możliwe jest przeprowadzenie ataku manin-the-middle (MITM) podczas opisywanego procesu negocjacji, co sprawi, że szyfrowanie będzie nieskuteczne. Więcej informacji znajduje się w sekcji 32.3.3.1.7.

Metody uwierzytelniania użytkowników.

Przed uzyskaniem nieograniczonego dostępu do zasobów wewnętrznych klient musi zidentyfikować i uwierzytelnić urządzenie kończące VPN. Najprostszą metodą uwierzytelniania jest hasło skojarzone z nazwą użytkownika jako identyfikatorem. Niektóre typowe metody sprawdzania poprawności poświadczeń użytkownika obejmują usługę zdalnego uwierzytelniania telefonicznego użytkownika (RADIUS), protokół Lightweight Directory Access Protocol (LDAP), natywną usługę Microsoft Active Directory (AD) lub Kerberos. Aby zwalczyć łatwość kradzieży lub odgadywania nazw użytkowników i haseł, większość dostawców udostępnia alternatywne lub uzupełniające mechanizmy uwierzytelniania. Istniejąca infrastruktura klucza publicznego (PKI) - patrz rozdziały 7 i 37 niniejszego podręcznika - otwiera możliwość korzystania z uwierzytelniania dwuskładnikowego poprzez wymaganie certyfikatu PKI użytkownika lub maszyny. Inną opcją wieloczynnikową jest użycie tokena kryptograficznego, takiego jak RSA SecurID lub karta inteligentna. Dostęp do zasobów wewnętrznych nie powinien być szeroko otwarty dla zdalnych użytkowników VPN, ani też nie należy wdrażać mechanizmu uniwersalnego dla wszystkich użytkowników VPN po uwierzytelnieniu. Często stosowana w sieciach VPN z dostępem zdalnym, autoryzacja użytkownika oparta na atrybutach rozszerzonego katalogu uwierzytelnionego użytkownika może dodatkowo kontrolować poziom dostępu do zasobu wewnętrznego. Na przykład na podstawie członkostwa w grupie lub roli użytkownika w katalogu LDAP łączność VPN powinna być przyznawana tylko określonym zasobom w sieci wewnętrznej. Ponadto pewnej klasie użytkowników lub działów należy przypisać zdefiniowaną, konkretną podsieć przestrzeni adresowej VPN. Dalsze zabezpieczenia, takie jak zapory ogniowe podrzędne lub zapory ogniowe oparte na hoście, mogą kontrolować dostęp użytkowników zdalnych do zasobów, do których zgodnie z polityką należy uzyskiwać dostęp spoza siedziby lub nie. Listy kontroli dostępu (ACL) stosowane do samego punktu końcowego VPN mogą ograniczać zasoby w sieci wewnętrznej, do których mogą uzyskiwać dostęp również użytkownicy zdalni. Użytkownicy VPN nigdy nie powinni być traktowani jako osoby o równych poziomach bezpieczeństwa; należy zastosować wszystkie możliwe punkty kontroli, zwłaszcza w środowisku kontroli dostępu opartym na rolach.

Wymagania dotyczące infrastruktury.

Sieci VPN dają możliwość korzystania ze Strefy Usług Zewnętrznych. Ponieważ urządzenie łączące VPN musi być połączone z Internetem, podział na strefy wymaga dwóch różnych sieci podłączonych do zapory. Zewnętrzny interfejs wychodzący z Internetu (niezaufany VPN) zawierałby tylko przychodzący i wychodzący zaszyfrowany ruch. Druga sieć (zaufana VPN) jest przeznaczona dla nieszyfrowanego ruchu przechodzącego do iz sieci wewnętrznej. Korzystając z tej zasady, zasada zapory ograniczyłaby zewnętrzne, przychodzące połączenia do urządzenia połączeniowego VPN przy użyciu tylko kilku wymaganych protokołów. Zasada zapory ograniczyłaby wszystkie połączenia zewnętrzne do nieszyfrowanej sieci, jednocześnie umożliwiając uwierzytelnionym klientom VPN odpowiedni poziom dostępu do sieci wewnętrznej. Ta nieszyfrowana sieć również zapewnia punkt kontroli bezpieczeństwa, który jest niezakłócony przez szyfrowanie.

Wymagania dotyczące dostępu do sieci.

Sieci VPN z dostępem zdalnym IPsec i TLS / SSL zapewniają bezpieczny dostęp zdalny, ale każda z nich wiąże się z unikalnymi wyzwaniami i możliwościami.

IPsec

Sieci VPN IPsec zazwyczaj zapewniają pełny dostęp do sieci wewnętrznej po pomyślnym nawiązaniu połączenia i uwierzytelnieniu. Implementacje VPN klienta IPSec wykorzystujące protokół IP 50 (ESP) lub protokół IP 51 (AH) nie zachowują się dobrze za urządzeniem NAT, co często ogranicza użyteczność dla użytkowników w hotelach, kawiarniach itp. Jednak skonfigurowanie protokołu IPsec do korzystania z transwersalnego NAT przez połączenie UDP lub TCP może obejść pierwotne ograniczenia. Możliwe jest również ograniczenie dostępu do wewnętrznych hostów i sieci za pomocą zasad RADIUS, urządzenia połączeniowego VPN i / lub zasad zapory. Jedną z kwestii, która wpływa na ruch klientów, jest Split Tunneling. Po włączeniu Split Tunneling tylko ruch przeznaczony dla sieci wewnętrznej przepływa przez zaszyfrowany tunel. Ruch sieciowy skierowany do Internetu przebiega najbardziej bezpośrednią trasą zamiast przechodzić przez tunel. Może to pomóc w zmniejszeniu przepustowości, ponieważ nie ma zbędnego ruchu przepływającego przez tunel. Jednak główną wadą jest utrata możliwości inspekcji ruchu sieciowego związanego z Internetem.

TLS / SSL

Oryginalna implementacja TLS / SSL VPN była daleka od swojego poprzednika IPsec. Te wczesne połączenia VPN koncentrowały się na przejściach sieciowych do określonych hostów i protokołów, a także na prymitywnym, trudnym do skonfigurowania portalu zawierającym proste łącza do wewnętrznych udziałów plików i witryn internetowych. Koncepcja portalu dotycząca zdalnego dostępu jest unikalna dla TLS / SSL VPN. Obecne portale są bardziej niezawodne i elastyczne, umożliwiając administratorowi dostarczanie określonych treści i dostępu do sieci w zależności od klasyfikacji użytkownika. Prawdziwym przełomem w sieciach VPN TLS / SSL było dopasowanie możliwości protokołu IPsec do umożliwienia pełnego dostępu do sieci, bez konieczności korzystania z pełnej sieci VPN dla klienta. Popularność tych sieci VPN gwałtownie wzrosła, ponieważ zmniejszają narzuty, zwykle dobrze zachowują się w sieciach z NAT i są łatwiejsze do skonfigurowania niż IPsec. Większość nowoczesnych implementacji SSL VPN obsługuje teraz również lekkiego klienta zdalnego dostępu, z których niektóre są wbudowane w obecne smartfony i tablety, które replikują w pełni zarządzane środowisko klient / serwer tradycyjnie używane we wdrożeniach sieci VPN dostępu zdalnego IPsec.

VPN typu SITE-TO-SITE.

Sieci VPN nie służą wyłącznie do zdalnego dostępu klienta. Sieci VPN typu Siteto-Site (S2S) zapewniają możliwość zaspokojenia potrzeb w zakresie komunikacji wewnętrznej. Istnieją technologie VPN, które mogą tworzyć siatkowe, wirtualne sieci rozległe (WAN), oprócz zapewnienia alternatyw dla tradycyjnych implementacji WAN.

Wieloprotokołowe przełączanie etykiet.

Multiprotocol Label Switching (MPLS) nadal zwiększa swoją dominację w świecie WAN. Chociaż nie jest to tradycyjna zaszyfrowana sieć VPN, zapewnia podobny rodzaj usługi. Ta sekcja nie obejmuje większości zawiłości MPLS, ponieważ wdrożenie musi spełniać wymagania organizacyjne oraz ponieważ każdy dostawca usług ma inną ofertę. Jednak MPLS ma kilka różnych, korzystnych cech. Cel, powód. MPLS tworzy siatkową, routowaną wirtualną sieć WAN na poziomie dostawcy usług. Sieć MPLS może wtedy swobodnie kierować pakiety bezpośrednio z jednego punktu końcowego WAN do drugiego w ramach swojej sieci wirtualnej. Witryny WAN mogą komunikować się bezpośrednio, zwiększając odporność sieci WAN, eliminując możliwość tworzenia jednej lokalizacji jako pojedynczego punktu awarii. Sieci MPLS mogą również zapewniać wiele poziomów jakości usług (QoS). QoS zapewnia możliwość ustalania priorytetów ruchu sieciowego, umożliwiając niektórym protokołom większą przepustowość w okresach wysokiego wykorzystania. Możliwe jest również ustanowienie tuneli IPsec za pośrednictwem sieci MPLS w celu zwiększenia poufności przechodzących danych. Wymagania. Podobnie jak w przypadku wszystkich technologii routingu WAN, sprzęt i oprogramowanie routingu muszą obsługiwać niezbędne protokoły routingu i / lub MPLS. Ponadto usługodawca musi już mieć dostępną technologię. Przejście na MPLS może wymagać znaczącej przebudowy istniejącej infrastruktury routingu

Zdalne sieci VPN.

Innym powszechnym zastosowaniem sieci IPsec VPN jest komunikacja międzylokacyjna (site-to-site, S2S) przez Internet.

Cel: Chociaż różnorodność geograficzna zapewnia organizacji bliższy kontakt z klientami i materiałami, tradycyjne wdrożenia sieci WAN mogą być niedostępne lub niepraktyczne. Sieci VPN dla zdalnych witryn zapewniają możliwość wypełnienia tej luki.

Alternatywna sieć WAN :. Uruchomienie tradycyjnego połączenia WAN (np. T1/T3, Metro Ethernet itp.) w wydzierżawionej lub posiadanej lokalizacji może być nieopłacalne. Ponadto nawet linia dzierżawiona o niższej przepustowości może być zawyżona i niewystarczająca, aby zapewnić bezpośrednią łączność WAN z małym oddziałem. Ten typ sieci VPN S2S może zapewnić niezbędny poziom łączności bez wysokich kosztów dzierżawionej linii. Ponieważ ta sieć VPN S2S będzie podróżować przez połączenie internetowe, może być możliwe zapewnienie wyższej przepustowości za tę cenę. Jednak zwiększona przepustowość może być niekorzystna od mniej przewidywalnej wydajności sieci, takiej jak brak kompleksowej usługi QoS.

Kopia zapasowa: S2S VPN przez Internet jest również alternatywnym sposobem tworzenia kopii zapasowych WAN. Chociaż komórkowa karta zapasowa może zapewnić większą przepustowość przy niższym koszcie niż cyfrowa sieć zintegrowanych usług (ISDN), sieci komórkowe zwykle mają większe opóźnienia i mogą być niewykonalne w zależności od lokalizacji budynku w stosunku do wieży komórkowej lub dostawcy. W przypadku odizolowanych lokalizacji połączenie satelitarne może być wykonalne, ale zazwyczaj ma jeszcze większe opóźnienie niż karta komórkowa. Rozwiązania te mogą być niewystarczające, jeśli witryna wymaga intensywnego dostępu do systemów i informacji w sieci WAN. S2S VPN przez Internet zapewnia większą przepustowość przy użyciu istniejącego sprzętu. Połączenie S2S zapewnia dodatkową nadmiarowość, zapewniając rezerwowe łącze routowalne. W

przypadku prawidłowej architektury lokacja powinna odnotowywać niewielką lub żadną awarię w przypadku awarii podstawowego łącza sieci WAN.

Połączenia dostawcy/partnera: Potrzeby biznesowe mogą wymagać połączenia sieci wewnętrznej z siecią dostawcy/partnera. Niezbędne jest odpowiednie planowanie, konfiguracja, konserwacja i monitorowanie tych połączeń, aby zapewnić, że żadna ze stron nie wprowadzi negatywnej sytuacji prowadzącej do kompromitacji i/lub utraty informacji. Ta konfiguracja zazwyczaj znajduje się za GSD, aby kontrolować dostęp tylko do niezbędnych protokołów, sieci i systemów. Jednak w zależności od niezbędnych protokołów (np. Remote Desktop Protocol lub RDP) śledzenie tego, co się stąd dzieje, może być trudne. System RDP może działać jako punkt wyjścia do innych części sieci, niekoniecznie chronionych na tym samym poziomie, na jakim mogą istnieć w sieci wewnętrznej.

Wymagania: Zdalne sieci VPN wymagają połączenia z Internetem, a także punktów końcowych obsługujących VPN i szyfrowanie. Typowe wdrożenie S2S może odbywać się między dwoma routerami. Inne potencjalne wdrożenia obejmują router do urządzenia zabezpieczającego bramy (GSD) z obsługą VPN lub z GSD do GSD.

Rozważania dotyczące zapewnienia informacji.

Chociaż zdolność ludzi i zdalnych lokalizacji do łączenia się z zasobami wewnętrznymi zapewnia mobilność i zwiększa produktywność, organizacja musi dokładnie rozważyć zastrzeżenia związane z zapewnieniem informacji. Każda realizacja będzie miała swoją unikatowość wymagań, ale rozwiązanie głównych problemów przedstawionych w kolejnych sekcjach może zapewnić bardziej świadome decyzje.

Uwagi dotyczące zdalnego dostępu do sieci VPN.

Sieci VPN z dostępem zdalnym stwarzają największe ryzyko narastająco. Wszystkie niekontrolowane sieci zasługują na traktowanie jako niepewne, a przez to wrogie środowiska obliczeniowe. Ponieważ istnieje niepewność co do bezpieczeństwa sieci, z której system użytkownika końcowego będzie się łączyć, konieczne jest, aby host dysponował wystarczającymi mechanizmami samoobrony, aby zrekompensować utratę dodatkowych dostarczonych warstw ochrony w głąb przez sieć wewnętrzną. To zrozumienie będzie wymagało od administratorów bezpieczeństwa skupienia się na niezbędnych środkach ostrożności w celu ochrony wszystkich systemów organizacji.

Wierność urządzenia mobilnego.

Ponieważ nie ma absolutnej kontroli, gdy systemy mobilne opuszczają granice sieci wewnętrznej, wierność urządzenia mobilnego jest problemem. Ryzyko naruszenia bezpieczeństwa na każdym poziomie — od fizycznego, przez system operacyjny, po aplikacje i nie tylko — może narazić sieć wewnętrzną na zwiększone ryzyko podczas sesji sieci VPN. ? ? ? ???? Istnieje kilka sposobów na zmniejszenie prawdopodobieństwa utraty wierności. Zabezpieczenia mogą obejmować dowolną kombinację oprogramowania zabezpieczającego opartego na hoście (np. zapora, ochrona przed złośliwym oprogramowaniem, zapobieganie włamaniom), aktualne poziomy poprawek i bezpieczne konfiguracje. Właściwe wdrożenie i konfiguracja tych środków ochrony pomoże zmniejszyć możliwość naruszenia bezpieczeństwa. Nawet jeśli wierność urządzenia jest akceptowalna podczas początkowego połączenia, nie gwarantuje to, że ten stan nie zmieni się w późniejszym czasie podczas połączenia. Inną metodą zapewnienia kondycji urządzenia jest kontrola dostępu do sieci (NAC). NAC zapewnia możliwość odpytywania łączącego się urządzenia przed i podczas połączenia w celu określenia takich informacji, jak poziomy poprawek, stan zabezpieczeń i złośliwe oprogramowanie rezydujące w pamięci . Niestety NAC to nie tylko propozycja typu plug-and-play. Istnieje wiele innych implikacji i wymagań,

takich jak określenie, co należy ocenić i/lub wyegzekwować, wdrożenia wbudowane lub pasywne oraz rozwiązania oparte na kliencie lub rozwiązania bezklienckie, związanych ze skutecznym wdrażaniem NAC w dowolnym punkcie sieci.

Zarządzanie klientem VPN.

Administracja klientem odgrywa kluczową rolę w sukcesie rozwiązania VPN. Protokół IPsec wymaga użycia aplikacji po stronie klienta lub mechanizmu wbudowanego systemu operacyjnego. Główne implikacje tego obejmują konfigurowanie i utrzymywanie klienta. Zawiłości związane z instalacją na twardym kliencie obejmują konieczność uzyskania lokalnych uprawnień administracyjnych, potencjalną interakcję użytkownika i radzenie sobie z uszkodzoną aplikacją kliencką VPN. Podobnie jak w przypadku wszystkich innych aplikacji, aktualizacje są konieczne ze względu na nowe ulepszenia, nieobsługiwane starsze wersje i luki w zabezpieczeniach. Zgodnie z celem minimalizacji negatywnych doświadczeń użytkowników administratorzy potrzebują sposobu na aktualizację oprogramowania klienckiego bez interakcji z użytkownikiem lub bez skutków ubocznych. Jednym z podstawowych pytań jest ustalenie, czy dostawca VPN ma mechanizm wypychania konfiguracji i innych aktualizacji oprogramowania klienckiego podczas połączenia. Bez tej funkcjonalności trudniej jest zmienić parametry po stronie klienta. Na przykład sieć VPN korzystająca ze wstępnie udostępnionego klucza do uwierzytelniania VPN zostaje na stałe zakodowana w konfiguracji oprogramowania VPN. To sprawia, że trudno jest go zmienić bez konieczności wprowadzenia przez użytkownika końcowego nowego klucza, a ponadto jest to droga do kompromisu, jeśli klucz można odzyskać. Klienci TLS/SSL VPN nie mają tych samych pułapek, co zarządzanie klientami IPsec. Zamiast twardego klienta TLS/SSL VPN zwykle używa małego dynamicznego klienta opartego na Javie lub ActiveX lub lekkiej instalacji specyficznej dla systemu operacyjnego. W niektórych systemach VPN administrator może mieć możliwość pozostawienia rezydenta dynamicznego klienta lub usunięcia go po rozłączeniu. Jeśli klient ulegnie uszkodzeniu, użytkownik może usunąć kontrolkę i zostanie ona automatycznie pobrana przy następnym udanym połączeniu. Pozostanie rezydentem dynamicznego klienta ma dwie zalety. Po pierwsze, może to zapewnić możliwość posiadania lokalnego, zaszyfrowanego obszaru roboczego do przechowywania dokumentów roboczych i innych plików lub zapewnienia dostępu do innych zasobów. Po drugie, dzięki temu system zdalny nie musi pobierać klienta przy każdym połączeniu. Klient TLS/SSL ma również tę zaletę, że zawsze sprawdza, czy klient rezydentny jest aktualny. Jeśli nie, system VPN wymusi pobranie najnowszego klienta, pomagając zminimalizować zarządzanie po stronie klienta. Niezbędne jest również odpowiednie monitorowanie zdalnych sieci VPN. Zhakowane połączenie VPN lub dane uwierzytelniające są niezwykle niebezpieczne i stają się coraz bardziej popularnym celem atakujących. Organizacje powinny monitorować dzienniki i połączenia pod kątem podejrzanej aktywności i mieć wdrożone procedury dotyczące takich problemów. . Na przykład, jeśli identyfikator użytkownika loguje się z głównego biura w Kalifornii, a mniej niż dwie godziny później ten sam identyfikator użytkownika loguje się z drugiego końca świata, prawdopodobnie drugie połączenie nie jest zamierzone lub legalne. Dotyczy to zwłaszcza środowisk z jednokrotnym logowaniem (SSO)

Ochrona Urządzenia VPN.

Sedno możliwości świadczenia usług VPN kręci się wokół istniejącej infrastruktury bezpieczeństwa sieci i ma bezpośrednie implikacje dotyczące ochrony obwodu, ponieważ urządzenia łączące VPN muszą być skierowane do Internetu i do wewnątrz. Urządzenia te muszą również być zgodne z zewnętrzną strefą serwisową omówioną w rozdziale 26 niniejszego podręcznika. Samo urządzenie jest kolejną częścią ogólnego profilu bezpieczeństwa sieci. Ważne jest, aby usunąć wszystkie dodatkowe narażenia. Podstawową metodą ochrony jest skonfigurowanie zapory tak, aby zezwalała na dostęp tylko do niezbędnych portów na urządzeniu VPN. Wszystkie niepotrzebne protokoły, usługi i opcje konfiguracyjne powinny zostać wyłączone. Jeśli narzędzie do zarządzania siecią używa protokołu ICMP

i/lub SNMP do monitorowania urządzenia VPN, reguły zapory lub wbudowane listy ACL powinny zezwalać na dostęp do tych protokołów tylko z określonego zestawu monitorujących hostów. Chociaż rozpoznanie sieci i ataki są nadal możliwe na tych portach, metoda ta drastycznie zmniejsza profil ataku. Dostęp do urządzeń administracyjnych nigdy nie powinien korzystać z niezabezpieczonych protokołów, takich jak Telnet, FTP lub HTTP. Zamiast tego administracja powinna odbywać się tylko przy użyciu odpowiednio skonfigurowanych zaszyfrowanych protokołów, takich jak Secure Shell (SSH) i Hypertext Transfer Protocol Secure (HTTPS). Dostęp administracyjny powinien być chroniony co najmniej nazwą użytkownika i silnym hasłem, a jeszcze lepiej dodać uwierzytelnianie dwuskładnikowe za pomocą certyfikatu lub tokena połączonego z kodem PIN lub hasłem. Aby zminimalizować dostęp administracyjny, tylko określone sieci lub hosty powinny mieć bezpośredni dostęp do Konsoli administracyjnej, a jeśli to możliwe, nigdy nie wolno im zezwalać na żadne interfejsy internetowe. Aby jeszcze bardziej zredukować narażenia administracyjne, możliwe jest użycie hosta przeskoku dla wszystkich administratorów. Jednak stwarza to możliwość pojedynczego punktu awarii administracyjnej, jeśli host skoku nie jest dostępny.

Opcje kryptograficzne.

Bez dokładnej kontroli protokołów kryptograficznych VPN można wybrać kombinację, która stwarza dodatkowe ryzyko naruszenia bezpieczeństwa lub ujawnienia informacji. Siła i właściwa implementacja ochrony kryptograficznej tunelu VPN jest niezbędna do ochrony danych i musi być wystarczająca do spełnienia wymagań bezpieczeństwa organizacji. Wybór dostępnych protokołów kryptograficznych dla IPsec następuje podczas negocjacji IKE. Zestaw szyfrów określa, które protokoły kryptograficzne są dostępne do ochrony sesji VPN. Na przykład, jeśli 3DES i SHA1 są uważane za niewystarczającą ochronę, te i wszystkie inne słabsze alternatywy muszą zostać usunięte z negocjowalnych opcji IKE lub zestawu szyfrów. Gwarantuje to, że niekompatybilni klienci nie mogą się połączyć, a podczas sesji VPN używane są tylko wystarczające zabezpieczenia.

Kontrola ruchu.

Kontrola ruchu sieciowego odgrywa kluczową rolę w utrzymaniu bezpieczeństwa sieci wewnętrznej. Ponieważ celem sieci VPN jest zapewnienie bezpiecznego transportu danych, stanowi to przeszkodę przy próbie oceny przychodzącego, zaszyfrowanego ruchu. Inspekcja ruchu sieciowego może wystąpić na urządzeniu łączącym VPN lub po niezaszyfrowanej stronie prowadzącej do sieci wewnętrznej. Chociaż ruch sieciowy jest o krok bliżej sieci wewnętrznej, stanowi to ważny punkt kontroli, w którym można wykrywać i chronić przed złośliwym ruchem. Niektóre urządzenia VPN i GSD mogą umożliwiać przeglądanie danych w tunelu, ocenę ruchu sieciowego (zapewniając punkt rozwiązywania problemów) i sprawdzanie danych przed przekazaniem do sieci nieszyfrowanej. Jednak wykonanie całej inspekcji urządzenia VPN może mieć znaczący wpływ na wydajność.

Moc obliczeniowa.

Szyfrowanie i odszyfrowywanie tuneli VPN wymaga odpowiedniej mocy obliczeniowej. Ten problem nasila się wraz ze wzrostem liczby klientów. W sytuacjach, w których jest tylko kilku klientów zdalnego dostępu, możliwe jest użycie routera do zakończenia połączeń VPN i świadczenia usług bezpieczeństwa. Im większa liczba klientów zdalnego dostępu, tym większe zapotrzebowanie na dedykowane urządzenia VPN (w tym GSD). Możliwe jest zainstalowanie sprzętowych akceleratorów szyfrowania w celu przeniesienia obliczeń kryptograficznych i zarządzania ze współdzielonego procesora na dedykowane urządzenie przetwarzające w routerze lub GSD, zmniejszając w ten sposób wymagania przetwarzania tych jednostek. Większe organizacje mogą mieć tysiące jednoczesnych użytkowników, co wymaga wielu urządzeń VPN.

Przechwytywanie.

Ponieważ sesje VPN przechodzą przez niekontrolowane sieci, złośliwi aktorzy mogą przechwycić zaszyfrowaną komunikację; jednak protokół datagramowy leżący u podstaw TCP/IP sprawia, że przechwytywanie sekwencyjnych pakietów jest trudne wszędzie poza źródłem i miejscem docelowym sesji. Jeśli atakujący zdoła przechwycić strumień danych, coraz bardziej prawdopodobne jest, że złamią zaszyfrowaną komunikację przy użyciu rozproszonych środowisk obliczeniowych z przetwarzaniem masowo równoległym. Jednak bardziej praktyczną metodą jest atak MITM podczas ustanawiania sesji VPN. Zarówno sieci VPN IPsec, jak i TLS/SSL są potencjalnie podatne na ataki MITM. Ataki MITM zwykle rozpoczynają się od złośliwego aktora w tej samej sieci co ofiara i przeprowadzają atak zatruwający protokołem ARP (Address Resolution Protocol), aby cały ruch przepływał przez system aktora przed przekazaniem go do reszty sieci. Główny wektor IPsec MITM to klucz wstępny (zazwyczaj nazwa grupy i hasło) do uwierzytelniania samego połączenia IPsec. Ten klucz jest zazwyczaj łatwy do odzyskania z plików konfiguracyjnych klienta VPN, chociaż takie podejście wymaga od złośliwego aktora wykorzystania dostępu po stronie klienta w celu ustalenia tych informacji. Po ustaleniu nazwy grupy i hasła narzędzie takie jak Fiked będzie emulować urządzenie końcowe VPN, uwierzytelniać połączenie IPsec i gromadzić dane uwierzytelniające użytkownika podczas próby uwierzytelnienia w celu uzyskania dostępu do pełnego połączenia VPN. Chociaż ten krok nie narusza poufności danych w ruchu, zapewnia podmiotowi możliwość dowolnego łączenia się z siecią wewnętrzną za pomocą zebranych danych uwierzytelniających. Istnieje możliwość obrony przed tym atakiem przy użyciu certyfikatu klienta lub komputera do uwierzytelniania IPsec. Możliwość naruszenia poufności TLS/SSL ze względną łatwością stała się rzeczywistością w 2009 roku wraz z wprowadzeniem SSLStrip. SSLStrip wykorzystuje atak zatrucia ARP polegający na przechwyceniu żądań klientów w celu użycia TLS/SSL. Po przechwyceniu narzędzie nawiąże prawidłowe sesje TLS/SSL z serwerem i utworzy przepisaną, niezaszyfrowaną sesję HTTP z klientem. Ta metoda nie powoduje wyświetlenia komunikatu o błędzie certyfikatu, który może ostrzec użytkownika o problemie z połączeniem. Narzędzie korzysta również z favicon kłódki, aby oszukać użytkownika, aby uwierzył, że połączenie jest bezpieczne, mimo że adres URL w rzeczywistości korzysta z protokołu HTTP, a nie HTTPS. Możliwe jest złagodzenie tego ataku, zezwalając tylko na bezpośrednie połączenia TLS/SSL zamiast przekierowywania z HTTP na HTTPS. Ponadto wcześniej ustanowione sesje TLS/SSL nie są podatne na ten atak.

Uwagi dotyczące Site-to-Site VPN

Projektowanie infrastruktury.

MPLS może być całkowitą zmianą w funkcjonowaniu sieci WAN, a także wprowadzać problemy związane z rozwiązywaniem problemów i bezpieczeństwem. Ponieważ sieć MPLS może zapewnić funkcjonalność kraty typu „dowolny z każdym”, trudniej jest rozwiązywać problemy z siecią. W topologii sieci WAN typu hub-and-spoke możliwe jest wdrożenie centralnie zlokalizowanych sond w celu monitorowania i rozwiązywania problemów z siecią WAN. Jest mało prawdopodobne, aby organizacje korzystające z MPLS w wielu lokalizacjach zainwestowały czas i pieniądze na wdrożenie tego typu monitorów we wszystkich lokalizacjach. Usługodawca może jednak być w stanie świadczyć dodatkowe usługi, które zapewniają tego typu możliwości rozwiązywania problemów za dodatkową opłatą. Sieci MPLS zwiększają również ogólne obciążenie związane z bezpieczeństwem sieci, wymagając zwiększenia liczby urządzeń zabezpieczających sieć w celu zapewnienia ochrony w każdym indywidualnym miejscu. Dzieje się tak głównie dlatego, że witryny mogą nawiązywać bezpośrednią komunikację zamiast najpierw iść do węzła. MPLS oddaje bezpieczeństwo infrastruktury WAN w ręce dostawcy usług.

Upewnij się, że dostawca MPLS ma solidną sieć i ścisłe procesy oddzielania sieci MPLS. Dodatkową ochroną przed błędami po stronie dostawcy jest wdrożenie zabezpieczenia routingu Border Gateway Protocol (BGP)23, w którym obie strony połączenia będą uwierzytelniać się, zanim staną się częścią tabeli routingu. Sieci VPN dla lokalizacji zdalnych stwarzają dodatkowe ryzyko, umieszczając Internet bezpośrednio w sieci wewnętrznej w lokalizacjach zdalnych. Jeśli Internet łączy się bezpośrednio z routerem witryny, istnieje kilka opcji ochrony. Lista ACL może ograniczyć komunikację do tego interfejsu tylko przez drugą stronę połączenia VPN w lokacji zdalnej. Inną opcją byłoby włączenie dodatkowych funkcji bezpieczeństwa na routerze. Może to jednak wymagać uaktualnienia kodu i zwiększyć wymagania dotyczące przetwarzania na routerze. Bezpieczniejszą, ale kosztowniejszą opcją byłoby wdrożenie GSD, który zapewnia usługi bezpieczeństwa i VPN, tworząc dodatkową kolejną warstwę ochrony między Internetem a siecią wewnętrzną. Wielopunktowe sieci VPN są również ważnym czynnikiem konstrukcyjnym. Tam, gdzie stało się to powszechne, jeśli nie jest to konieczne, w przypadku wysoce dostępnych, szerokopasmowych połączeń VPN, typowy projekt sieci VPN z lokalizacją centralną lub hub-and-spoke może nie być pożądany. Wiele projektów opiera się na punkcie centralnym w celu ustanowienia siatki połączeń VPN typu jeden-do-wielu. Jeśli jednak centralny punkt jest niedostępny, cała siatka VPN nie działa. Wielopunktowe sieci VPN usuwają zależność od centralnego punktu końcowego VPN. Jeśli centralny punkt końcowy stanie się tymczasowo niedostępny, inne punkty końcowe są w stanie komunikować się i negocjować połączenia między sobą bez obecności węzła centralnego (lub głównego). Dzięki temu pozostała część sieci VPN pozostaje operacyjna i przekierowuje ruch do innych punktów końcowych, które w innym przypadku byłyby niedostępne bez centralnego punktu końcowego.

Koszt

MPLS zwiększa koszty na wielu frontach. Obejmują one koszt nowych lub przekonwertowanych obwodów i dodatkowych usług, takich jak QoS lub możliwości monitorowania. Ponadto sprzęt obsługujący sieć musi być w stanie obsługiwać nową architekturę MPLS i routingu. Przeprojektowanie infrastruktury routingu sieciowego może również wymagać znacznej inwestycji czasowej. Sieci VPN S2S wykorzystujące urządzenia routujące wymagają wystarczającej mocy obliczeniowej (np. moduły pamięci RAM i szyfrowania o dostępie swobodnym). W niektórych przypadkach uzyskanie poziomu kodu obsługującego szyfrowanie może być droższe. Koszt wdrożeń S2S VPN przy użyciu GSD rośnie wraz ze wzrostem liczby usług bezpieczeństwa, a także liczby klientów, z którymi można się połączyć. Wdrażanie GSD w lokalizacjach zdalnych wiąże się nie tylko z kosztami pieniężnymi, ale także wyższymi kosztami administracyjnymi zarządzania tym nowym elementem infrastruktury routingu i bezpieczeństwa. .

Dostępność.

VPN to mniej wygoda, a bardziej konieczność. Awaria VPN może spowodować poważne zakłócenia dla wysoce mobilnej siły roboczej. Nawet w przypadku warstw wyeliminowanie wszystkich punktów awarii może być trudne ze względu na związane z tym koszty. Jeśli organizacja uważa VPN za konieczność, rozwiązania o wysokiej dostępności są wymogiem. Jednym z możliwych rozwiązań jest równoważenie obciążenia połączeń przychodzących w celu dystrybucji ich na wiele urządzeń. Jeśli jedno urządzenie ulegnie awarii, pozostałe urządzenia będą nadal obsługiwać wcześniej podłączonych klientów i zapewnią miejsce do połączenia dla nowych klientów. Inną opcją jest przełączanie awaryjne aktywne/w trybie gotowości: Jeśli jedno urządzenie ulegnie awarii, drugie będzie dostępne dla nowych połączeń. Korzystnym sposobem byłoby zreplikowanie przez aktywny element informacji o połączeniu do elementu rezerwowego. Jeśli aktywny element członkowski ulegnie awarii, członek rezerwowy może kontynuować obsługę istniejących tuneli VPN i akceptować nowe połączenia. Cała ta strategia opiera się również na tym, że główne punkty połączeń VPN mają nadmiarowe łącza internetowe,

nieprzerwaną energię elektryczną, kontrolę środowiska i infrastrukturę sieci zaplecza. VPN oparty na chmurze staje się również popularną alternatywą zapewniającą podstawową lub zapasową dostępność zdalnego dostępu VPN. Usługi te wyeliminowały potrzebę budowania i utrzymywania przez organizację dedykowanej infrastruktury VPN. Zamiast tego Sieć może być logicznie rozszerzona na dostawcę chmury, który integruje te połączenia z rozproszoną, wysoce skalowalną infrastrukturą VPN hostowaną w chmurze. Ta klasa usług jest popularna, gdy istnieje wiele geograficznie zróżnicowanych punktów końcowych VPN lub zdalnych użytkowników, w których konieczne jest niewielkie opóźnienie lub krytyczny jest czas pracy bez przestojów.

Implikacje nieuchwytnych sieci VPN.

VPN i usługi podobne do VPN występują w większej liczbie miejsc, niż większość ludzi zdaje sobie sprawę. Te niewidoczne sieci VPN obejmują zarówno legalne usługi VPN, takie jak GotoMyPC25, jak i złośliwe sieci VPN, takie jak kanały dowodzenia i kontroli botnetów oraz tunele zwrotne. Chociaż witryny VPN, takie jak GoToMyPC, mogą być przydatne, decyzja, czy jest to akceptowalny sposób zdalnego dostępu ad hoc, należy do organizacji. Niektóre z kluczowych kwestii, które należy wziąć pod uwagę w przypadku tego typu usługi VPN, polegają na omijaniu wewnętrznych kontroli bezpieczeństwa, takich jak inspekcja pakietów i zawartości, a strona trzecia tworzy połączenie VPN i zarządza nim. Złośliwe sieci VPN są źródłem ciągłych obaw. Kanały dowodzenia i kontroli botnetu mogą używać szyfrowania w celu ominięcia zabezpieczeń sieciowych, które chronią informacje. Tunel zwrotny działa poprzez przekierowanie ruchu sieciowego przeznaczonego dla portu nasłuchującego do tego samego portu na innym hoście. Na przykład, jeśli skompromitowany serwer FTP miał aktywny tunel zwrotny, każdy użytkownik próbujący połączyć się z tym serwerem FTP przekierowałby na inny serwer FTP. Poza teorią skompromitowanego hosta, złośliwi ludzie już w sieci wewnętrznej mogą nawiązać wychodzące połączenie VPN w celu ukrycia ruchu sieciowego. Najbardziej nieuchwytne ze wszystkich są aplikacje, które zapewniają wbudowane usługi podobne do VPN. Sieci peer-to-peer (P2P) tunelują udostępnianie plików za pomocą zastrzeżonych i szyfrowanych protokołów. Skype ma nie tylko możliwość tworzenia zaszyfrowanych połączeń głosowych, ale także funkcje podobne do VPN, które umożliwiają szyfrowane przesyłanie plików. Ochrona sieci powinna być w stanie wykryć konfigurację tych sesji i zatrzymać je przed zakończeniem połączenia. Od organizacji zależy opracowanie wewnętrznych zabezpieczeń sieci i zasad niezbędnych do ochrony przed wszystkimi nieuchwytnymi sieciami VPN.

Wpływ IPv6.

Masowa migracja do IPv6 nadal postępuje wolniej niż można by się spodziewać, mimo że IPv6 został opracowany pod koniec lat 90 i alokacja ostatnich dostępnych bloków adresów IPv4 do regionalnych rejestrów internetowych nastąpiła w 2011 r. Chociaż większość organizacji nadal ignoruje ryzyko i konsekwencje opóźniania korporacyjnych planów przejścia na IPv6, prawdopodobnie protokół jest już w ich środowisku. Prawie wszystkie nowoczesne systemy operacyjne mają podwójne stosy sieciowe IPv4 i IPv6, zwykle domyślnie włączone i zazwyczaj domyślnie preferują IPv6. IPv6 i związane z nim technologie przejściowe mają określone konsekwencje dla sieci VPN. Bez wszechobecnej kompleksowej łączności IPv6 istnieje kilka technologii przejścia IPv6 (takich jak 6to4 i Teredo), które umożliwiają systemom obsługującym IPv6 na obu końcach tunelowanie komunikacji przez starsze sieci IPv4. Metoda 6to4 hermetyzuje pakiet IPv6 w ładunku pakietów protokołu IPv4 typu 41 i wymaga użycia routerów przekazujących wraz z co najmniej jednym globalnie przypisanym adresem IPv4. Teredo hermetyzuje pakiety IPv6 w ładunku datagramów UDP, a także wykorzystuje routery przekazujące. UDP pozwala na lepsze przechodzenie środowisk korzystających z NAT. Technologie te zmniejszają barierę w adopcji IPv6 poprzez zwiększenie dostępności usług obsługujących IPv6; jednak technologie te często nie są dobrze rozumiane ani zarządzane. Większość administratorów sieci i

zabezpieczeń boleśnie przekonuje się, że podczas pracy zgodnie z założeniami połączenie (VPN lub lokalne) z zasobem obsługującym protokół IPv6 za pośrednictwem technologii przejściowej może przekroczyć granicę organizacji więcej niż raz, powodując znaczne opóźnienia i przesyłając dane przez kilka przekaźników routery niekontrolowane przez organizację. Te technologie przejściowe mają poważny wpływ na bezpieczeństwo zarówno sieci lokalnej, jak i połączeń VPN - błędne konfiguracje i brak doświadczenia są najbardziej niebezpieczne. Bez prawidłowej konfiguracji (i testowania) obu punktów końcowych ruch IPv6 może obrać niezabezpieczoną ścieżkę przed (lub nawet po) wchodzeniu do tunelu VPN, narażając dane na jaw, a tym samym zagrożone. Dla administratorów sieci i użytkowników VPN niezwykle ważne jest posiadanie prawidłowej, przetestowanej konfiguracji IPv6, aby zapewnić, że ruch IPv6 (zarówno natywny, jak i tunelowany) przechodzi tylko przez zabezpieczony tunel VPN i nie przechodzi żadnego zamkniętego tunelu niekontrolowanego przez organizację. Jeśli to zagrożenie nie jest zarządzane, dane mogą być podatne na ataki, nawet jeśli organizacja uważa, że jej sieć VPN zapewnia dodatkowe bezpieczeństwo zdalnej lokalizacji lub pracownikowi. Te technologie przejściowe, z których wiele jest domyślnie włączonych, mają również tendencję do automatycznego konfigurowania tuneli i połączeń. Konfiguracja punktu końcowego, zwłaszcza na klienckich stacjach roboczych, musi być centralnie konfigurowana lub zarządzana, aby wyłączyć te automatyczne połączenia lub określić określone konfiguracje, tak aby niezamierzone tunele nie były konfigurowane. IPv6 ma również natywną obsługę IPsec (zarówno AH, jak i ESP) poprzez użycie nagłówków rozszerzeń (w przeciwieństwie do zastrzeżonych klientów IPsec), chociaż jego użycie jest opcjonalne. Konfiguracja i używanie IPsec w środowisku IPv6 wymaga takiej samej dyscypliny przy wyborze i konfiguracji opcji kryptograficznych jak IPv4. Możliwe jest również użycie IPv4 IPsec do ochrony tuneli technologii przejścia IPv6, ponieważ w przeciwnym razie nieszyfrowane sesje tunelowe byłyby podatne na przechwycenie i/lub manipulację bez tej ochrony. Obie te opcje są zazwyczaj źle rozumiane i często nieskonfigurowane na urządzeniach sieciowych i VPN. Organizacje powinny brać pod uwagę natywny protokół IPsec dla protokołu IPv6 dopiero po przeprowadzeniu dokładnej edukacji i procesu planowania.

DODATKI. Wraz ze wzrostem konieczności wygodnego dostępu do danych rosną wyzwania związane z zapewnieniem ochrony wymaganej do zabezpieczenia tego typu dostępu. .

Cele w zakresie zapewnienia informacji.

Zezwalanie podmiotom zewnętrznym na zdalny dostęp do danych wewnętrznych ma poważne konsekwencje dla zapewnienia informacji. Główne cele ekstranetów w zakresie zapewniania informacji to ochrona wspólnych zasobów informacyjnych, zapobieganie ujawnieniu informacji i minimalizowanie dodatkowych ryzyk.

Ochrona wspólnych zasobów informacyjnych: Duża część obecnego rynku bezpieczeństwa informacji koncentruje się na ochronie hostów i sieci przed zagrożeniami cyfrowymi. Chociaż utrata serwera lub części sieci niewątpliwie powoduje problemy, niektóre obszary mogą budzić większe obawy. Organizacje rozwijają i utrzymują przewagę konkurencyjną, manipulując zebranymi lub utworzonymi danymi w wartościowe i przydatne informacje. Zmniejszając ryzyko związane z dostępem z zewnątrz, zmniejsza się prawdopodobieństwo wystąpienia naruszenia bezpieczeństwa informacji.

Zapobieganie ujawnianiu informacji: koncepcja najmniejszych uprawnień jest niezbędna podczas projektowania dostępu do systemu. Nie można by oczekiwać, że analityk finansowy będzie miał dostęp do zastrzeżonych specyfikacji produktów. Te same koncepcje obowiązują podczas przypisywania dostępu do podmiotów zewnętrznych. Zarządzanie tożsamością zapewnia mechanizm odpowiedzialności za nadawanie uprawnień i monitorowanie akcji wydanych kont. Zarządzanie dostępem zapewnia mechanizm egzekwowania, który uniemożliwia tym kontom przeglądanie lub

zmienianie danych, które nie są wyraźnie potrzebne. Połączenie tych dwóch zasad zmniejsza ryzyko niewłaściwego lub nieoczekiwanego dostępu.

Zminimalizuj dodatkowe ryzyko: atakowanie systemów połączonych z Internetem nie trwa długo. Minimalizacja wektorów ataków z Internetu następuje od warstwy sieci do warstwy aplikacji. Serwery ekstranetowe nie są systemami uniwersalnymi. Zasady ochrony sieci powinny ograniczać dostęp do tych usług, tak aby społeczność internetowa miała dostęp tylko do określonych reklamowanych usług. Usługi ekstranetowe wymagają większej uwagi, ponieważ urządzenia zabezpieczające sieci wciąż nie są w stanie chronić protokołów i dostosowań rutynowo występujących w warstwie aplikacji.

Koncepcje ekstranetu.

Strefa usług zewnętrznych : Jak opisano w rozdziale 26 tego podręcznika, sieci ekstranetowe są kolejną okazją do korzystania z podziału na strefy, głównie dlatego, że ekstranety wymagają solidnej ochrony i intensywnie wykorzystują zasoby w innych strefach. Podział na strefy pozwala administratorom na bardziej szczegółowe informacje na temat usług dopuszczonych do sieci, a także zapewnienie innej lokalizacji dla dodatkowego mechanizmu bezpieczeństwa.

Architektura wielowarstwowa : Jeśli system ekstranetowy zapewnia wszystkie aspekty usługi, istnieje pojedynczy punkt awarii i kompromisu. Architektura N-Tier zapewnia możliwość dystrybucji różnych aspektów oferty usług do dodatkowych systemów. System ekstranetowy zapewni frontowy interfejs użytkownika; serwer aplikacji ułatwia logikę i przetwarzanie niezbędne do uzyskania dostępu do danych; a serwer bazy danych zaplecza przechowuje i dostarcza dane. Ponieważ serwer ekstranetu znajduje się w strefie usług zewnętrznych, zasady zapory muszą umożliwiać temu serwerowi łączenie się z serwerami następnej warstwy w sieci wewnętrznej. Jeśli to możliwe, ogranicz dostęp z serwera ekstranetowego do sieci wewnętrznej tylko do niezbędnych systemów i usług. Ta architektura pomaga stworzyć bardziej niezawodną infrastrukturę, która zmniejsza niepotrzebne narażenia.

Szyfrowanie TLS/SSL: Najbardziej widocznym znacznikiem szyfrowania TLS/SSL jest mała ikona złotej kłódki, która pojawia się w przeglądarce internetowej podczas łączenia się z serwerem za pomocą protokołu HTTPS. Gdy host próbuje połączyć się z serwerem ekstranetowym, przed rozpoczęciem zaszyfrowanej sesji następuje kilka kroków. Host łączący udostępnia parametry związane z SSL w celu negocjowania połączenia HTTPS z serwerem. Następnie serwer odpowiada, podając wynegocjowane parametry związane z SSL oraz certyfikat cyfrowy. Klient następnie używa certyfikatu do uwierzytelnienia serwera. Jeśli uwierzytelnianie się powiedzie, klient i serwer ustanawiają klucze szyfrowania używane do ochrony sesji i rozpoczynania zaszyfrowanej komunikacji.

Rodzaje dostępu do Extranetu.

Rodzaj systemów i usług, które można przenieść do ekstranetu, stale rośnie. Świadczenie usług ekstranetowych zawsze podlega potrzebom organizacji, a poniższe sekcje zawierają kilka typowych przykładów systemów ekstranetowych.

Udostępnianie informacji o dostawcach/partnerach: firmy przetrwają i rozwijają się dzięki przewadze konkurencyjnej i coraz częściej muszą dzielić się informacjami ze strategicznymi partnerami. Zapewniając dostęp do informacji wewnętrznych, partnerzy ci mogą lepiej zrozumieć i zaspokoić potrzeby organizacji. Systemy planowania zasobów przedsiębiorstwa (ERP) zawierają dane, które służą jako cyfrowa siła napędowa organizacji. W ekstranecie dostawcy i partnerzy biznesowi mogli mieć dostęp do pracy z informacjami przechowywanymi w systemie ERP.

Handel elektroniczny : Cyfrowe prowadzenie transakcji biznesowych może zwiększyć wydajność i obniżyć koszty. Handel elektroniczny występuje na poziomie biznesowym i konsumenckim. Firmy

mogą korzystać z elektronicznej wymiany danych (EDI), która umożliwia dwóm podmiotom wymianę standardowych, cyfrowych wersji dokumentów, takich jak zamówienie zakupu i płatności, bez interakcji człowieka. Ekstranet umożliwia partnerom biznesowym wymianę danych EDI bez udzielania dostępu do wewnętrznych serwerów, które faktycznie przetwarzają i przechowują dane. Konsumenci uzyskują dostęp do witryn handlu elektronicznego, aby przeglądać i kupować towary i usługi.

Wydajność pracowników: świadczenie usług ekstranetowych nie ogranicza się do partnerów biznesowych i konsumentów. Możliwe jest zwiększenie dostępu pracowników do określonych usług i systemów wewnętrznych poprzez umożliwienie dostępu bez konieczności pełnego połączenia VPN. Poczta e-mail to uniwersalne narzędzie biznesowe, a świadczenie usług poczty internetowej umożliwia pracownikom dostęp do poczty e-mail z niemal każdego miejsca na świecie na dowolnym urządzeniu z przeglądarką internetową. Pracownicy mogą uznać za pomocną możliwość dostępu i zmiany informacji o świadczeniach z domu. Może to być również okazja do umożliwienia dostępu do informacji intranetowych za pośrednictwem systemu zarządzania treścią.

Outsourcing : Przedsiębiorstwa, które nie posiadają wymaganej wewnętrznej wiedzy ludzkiej lub technologicznej, aby osiągnąć cele IT organizacji, od dawna szukają rozwiązań outsourcingowych, aby zaspokoić swoje potrzeby. Oprogramowanie jako usługa (SAAS) oferuje takie oferty, jak aplikacje biurowe, współpraca i poczta e-mail (np. Microsoft Office365) i CRM (np. salesforce.com). Infrastruktura i platforma jako usługa (odpowiednio IAAS i PAAS) zapewniają przechowywanie i przetwarzanie danych na żądanie (Amazon Web Services-S3/EC2 lub Rackspace Open Cloud). Każda z tych zlecanych na zewnątrz ofert wciąż dojrzewa i redefiniuje sposób, w jaki przedsiębiorstwa rozwijają, zarządzają i prezentują swoje informacje

Rozważania dotyczące zapewnienia informacji

Bezpieczeństwo techniczne.

Zabezpieczenie ekstranetu nie jest możliwe w pojedynczej warstwie lub punkcie sieci. Każda warstwa jest współzależna i wymaga określonych zabezpieczeń, aby zapewnić bezpieczeństwo sieci ekstranetowej.

Infrastruktura.

Ponieważ ekstranet znajduje się za GSD, środki bezpieczeństwa warstwy sieci są zwykle zabezpieczeniami napotykanymi w pierwszej kolejności.

Kontrola ruchu: Jak powtarzano w wielu częściach tego i innych rozdziałów, niektóre urządzenia zabezpieczające mają wyraźną niezdolność do oceny zaszyfrowanego ruchu sieciowego. Ekstranet może powodować dodatkowe problemy, ponieważ zaszyfrowana sesja może przejść od klienta bezpośrednio do serwera ekstranetu. Potencjalnie wymaga to przeprowadzenia inspekcji ruchu na serwerze ekstranetowym. Chociaż jest to możliwe, ta metoda zwiększy wymagania serwera dotyczące przetwarzania. Inną opcją jest zakończenie połączeń SSL na urządzeniu nadrzędnym. To urządzenie korzystałoby następnie z nieszyfrowanych protokołów po stronie niższej, komunikując się z rzeczywistym serwerem ekstranetowym. Ta metoda dodaje dodatkową warstwę złożoności podczas rozwiązywania problemów, ale może zwolnić serwer ekstranetowy z obciążeń związanych z szyfrowaniem i kontrolą bezpieczeństwa.

Ekspozycja na sieć wewnętrzną : chociaż naruszenie bezpieczeństwa serwera ekstranetowego jest znaczące, nie powinno zapewniać nieskrępowanego dostępu do zasobów wewnętrznych. Chociaż zasady zapory umożliwiają dostęp do określonych usług ekstranetowych z Internetu, zasady zapory

muszą również szczegółowo ograniczać dostęp z serwera ekstranetowego do systemów wewnętrznych.

Serwer.

Ochrona na poziomie serwera to prawdziwa pierwsza linia obrony. Mechanizmy zabezpieczeń warstwy sieciowej mają trudności z ochroną serwera, który reklamuje podatną na ataki usługę. Wzmacnianie systemu to podejście do zmniejszania ogólnego profilu ryzyka serwera. Nieistotne protokoły i usługi są wyłączane. System operacyjny (OS) może mieć dodatkowe parametry, takie jak uprawnienia do plików i kont, które dodatkowo zmniejszają profil ryzyka. Skrypt może pomóc w zapewnieniu, że te zmiany następują w spójny sposób. Jednym z dobrze znanych skryptów wzmacniających system jest Bastille Linux. Ze względu na złożoność systemów operacyjnych i aplikacji pojawią się luki w zabezpieczeniach. Najprostszą metodą naprawienia luk jest aktualizacja serwera za pomocą łatki. Ważne jest, aby przed wdrożeniem w środowisku produkcyjnym przetestować poprawki pod kątem niepożądanych skutków. Ta praktyka pomoże zmniejszyć ryzyko nieoczekiwanych wyników i przestojów. Opracowanie i wydanie poprawki może zająć sprzedawcom tygodnie lub miesiące. W niektórych przypadkach łatki innych firm będą dostępne dla niezałatanych, aktywnie wykorzystywanych luk w zabezpieczeniach. Chociaż możliwość korzystania z tych plastrów jest opcją, jest to niewskazane ze względu na brak możliwości weryfikacji ich integralności i bezpieczeństwa. Mimo że celem jest zminimalizowanie profilu ryzyka serwera za pomocą wszystkich tych środków, może być również konieczne zapewnienie dodatkowych zabezpieczeń na poziomie serwera, w tym zapory opartej na hoście i oprogramowania zapobiegającego włamaniom. . Te zabezpieczenia mają tę zaletę, że są kontekstowo świadome systemów operacyjnych i funkcji aplikacji, w przeciwieństwie do tych znajdujących się w warstwie sieci. Wirtualizacja jest już głęboko zakorzenionym aspektem infrastruktury serwerów wewnętrznych i ekstranetu. Chociaż wirtualizacja zapewnia ekonomię skali, umożliwiając działanie wielu systemów ekstranetowych na jednym serwerze lub klastrze, wiąże się to z wieloma implikacjami dotyczącymi bezpieczeństwa. Bez klastrowania pojedynczy punkt awarii występuje w przypadku awarii serwera fizycznego. Ponieważ przełącznik wirtualny kieruje większością ruchu warstwy 2 generowanego przez maszyny wirtualne, istnieje minimalna widoczność natywna i egzekwowanie bezpieczeństwa ruchu sieciowego generowanego między maszynami wirtualnymi. Egzekwowanie zabezpieczeń osadzone w maszynach wirtualnych jest coraz łatwiej dostępne w celu ochrony na poziomie hipernadzorcy. Ciągle pojawiają się również obawy o ucieczkę z sesji wirtualnych i umożliwienie nieautoryzowanego dostępu do innej sesji wirtualnej.

Zastosowanie.

Niektóre typowe luki w warstwie aplikacji obejmują przepełnienia bufora, wstrzykiwanie języka SQL (Structured Query Language) i skrypty międzylokacyjne (XSS). Przepełnienia bufora istniały kilkadziesiąt lat temu, ale nadal są ulubionym miejscem twórców szkodliwego kodu. Warunek ten istnieje, ponieważ aplikacja nie sprawdza prawidłowo granic pól wejściowych lub używa funkcji, które nie wykonują tego samego. Wstrzyknięcie SQL to złośliwa próba wstawienia zapytania SQL do żądań po stronie serwera. Nie sprawdzając i nie chroniąc przed tego typu atakiem, serwer zaplecza może zwrócić informacje żądane przez złośliwe zapytanie. XSS to rodzaj wstrzykiwania kodu, powszechnie używany do phishingu. Złośliwy gracz może wysłać niczego niepodejrzewającej osobie link, który przekierowuje część lub całą zawartość w inne miejsce. Luki w warstwie aplikacji mogą z łatwością pokonać nawet najbezpieczniejsze konfiguracje warstwy sieciowej. Aplikacje opracowane przez wielomiliardowe organizacje mogą być tak samo wrażliwe, jak aplikacje opracowane wewnętrznie w małym obiekcie. Deweloperzy muszą rozumieć i przestrzegać zasad bezpiecznego kodowania, aby zminimalizować liczbę i wagę luk w zabezpieczeniach aplikacji. Rozdziały 38, 39 i 52 w tym podręczniku

zawierają omówienie programowania i bezpieczeństwa aplikacji, a rozdziały 30 i 31 dotyczą bezpieczeństwa internetowego.

Polityki.

Ponieważ ekstranety zapewniają zewnętrznym podmiotom dostęp do wewnętrznych informacji i systemów, wskazane jest posiadanie polityki regulującej korzystanie z tych systemów. Polityka może zawierać informacje o wymaganiach, takich jak konieczność zawarcia umowy o zachowaniu poufności przed zezwoleniem partnerowi biznesowemu na dostęp do ekstranetu lub nakaz używania szyfrowania TLS/SSL dla całej komunikacji ekstranetowej. Polityki nie zapewniają aktywnego mechanizmu ochrony, ale określają oczekiwania podczas korzystania z systemów ekstranetowych i konsekwencje nieprzestrzegania tych wymagań.

Zarządzanie dostępem i tożsamością.

Zarządzanie dostępem ma kluczowe znaczenie dla zapewnienia, że tylko niezbędne i istotne informacje docierają do żądającego użytkownika. Uprawnienia nadane temu użytkownikowi będą dyktować dane, do których użytkownik może uzyskać dostęp i powinny być zgodne z koncepcją najmniejszych uprawnień. Zarządzanie tożsamościami zapewnia, że tylko odpowiednio uwierzytelnione jednostki mogą uzyskać dostęp do ekstranetu i systemów bazowych. Zazwyczaj użytkownik zewnętrzny uwierzytelni się przy użyciu nazwy użytkownika i hasła. Niestety jest to kiepski sposób na zweryfikowanie tożsamości podmiotu ze względu na łatwość kradzieży lub odgadnięcia haseł. Bardziej niezawodną metodą identyfikacji podmiotu zewnętrznego byłoby wymaganie uwierzytelniania wieloskładnikowego przy użyciu kombinacji nazwy użytkownika/hasła i wydanie użytkownikowi certyfikatu cyfrowego. Certyfikat stałby się wówczas częścią procesu łączenia i uwierzytelniania. Chociaż nie jest to niemożliwe, znacznie trudniej jest sfałszować i/lub ukraść certyfikat cyfrowy. Federated Identity Management (FIdM)31 to powszechna metoda zapewniania funkcji uwierzytelniania jednokrotnego logowania między co najmniej dwoma organizacjami partnerskimi. Protokoły, takie jak Security Assertion Markup Language (SAML)32, tworzą opartą na standardach metodę komunikacji i weryfikacji informacji uwierzytelniających dla każdej ze stron. Ze względu na zawiłe szczegóły FIdM w tym rozdziale wspomniano jedynie o jego potencjalnym wykorzystaniu jako mechanizmu uwierzytelniania usług ekstranetowych. Ponieważ każda organizacja federacyjna musi pokładać w sobie pewien poziom zaufania, ważne jest, aby przejść przez proces dokładnego planowania, aby zidentyfikować i złagodzić ryzyko związane z tą technologią. Rozdziały 28 i 29 niniejszego Podręcznika zawierają szczegółowe informacje na temat identyfikacji i uwierzytelniania.

Dostępność.

Systemy ekstranetowe są ważną częścią działalności biznesowej. Gdy dostęp do ekstranetu jest niedostępny, nie występują pewne transakcje, które mogą powodować problemy w punktach w całej organizacji. Dostępność Extranetu jest funkcją infrastruktury sieciowej i serwerowej. Pojedyncze połączenie internetowe ma domniemany pojedynczy punkt awarii, jeśli połączenie to zostanie przerwane. Jeśli infrastruktura sieciowa prowadząca do ekstranetu ma tylko jedną ścieżkę, którą należy podążać, staje się to kolejnym pojedynczym punktem awarii. Dodanie nadmiarowości do infrastruktury sieciowej, takiej jak drugie połączenie internetowe i dodatkowe ścieżki routingu, zmniejsza prawdopodobieństwo przestojów. Infrastruktury serwerowe mają również taki sam potencjał bycia pojedynczym punktem awarii. Zamiast tego, używając pojedynczego serwera do świadczenia usługi ekstranetowej, możliwe jest wdrożenie klastra serwerów i równoważenie obciążenia. Klaster będzie chronić dostępność usługi w przypadku awarii jednego lub większej liczby serwerów. Ponadto zapewnia to możliwość wykonywania konserwacji serwera z niewielkim lub zerowym wpływem na

dostępność. Równoważenie obciążenia pomaga zoptymalizować liczbę połączeń do każdego członka klastra.

Wpływ IPv6.

Największy wpływ IPv6 na ekstranet ma obsługa infrastruktury i aplikacji. Jak wspomniano wcześniej, systemy operacyjne i aplikacje muszą być w stanie akceptować, przetwarzać i odpowiadać na pakiety IPv6; infrastruktura routingu musi być w stanie komunikować się przy użyciu protokołu IPv6 natywnie lub za pośrednictwem mechanizmu tunelowania przejścia IPv6 (np. Teredo lub 6to4); i wreszcie, infrastruktura bezpieczeństwa musi być w stanie ocenić pakiety IPv6. Awaria któregokolwiek z nich sprawi, że ekstranet będzie podatny na ataki lub niedostępny.

UWAGI KOŃCOWE.

Sieci VPN i ekstranety mają wiele zaawansowanych funkcji, które mogą zwiększyć zdolność organizacji do prowadzenia i poprawy mobilności pracowników i funkcjonalności biznesowej. Wsparcie i wkład muszą pochodzić ze wszystkich poziomów organizacji, aby zapewnić, że systemy bezpiecznego dostępu zdalnego spełniają specyficzne potrzeby i oczekiwania organizacji. Co najważniejsze, systemy te muszą być zgodne i wzmacniać, a nie zmniejszać ogólny profil bezpieczeństwa organizacji.