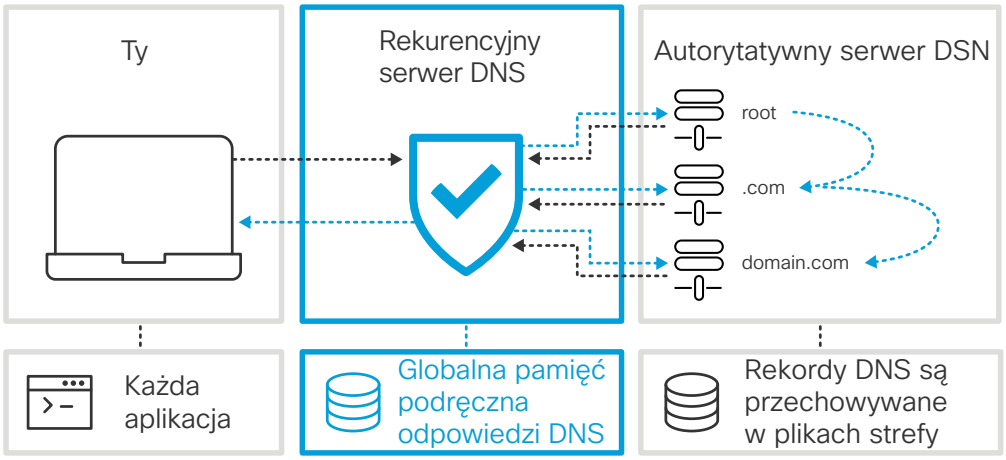
10 powodów, dlaczego ponad 15 000 przedsiębiorstw przekierowuje swoje serwery DNS do platformy Cisco Umbrella.

Większe bezpieczeństwo, niezrównana niezawodność i prędkość działania rekurencyjnych serwerów DNS w porównaniu z usługami dostawców Internetu lub lokalnymi serwerami DSN

Zespół obsługujący platformę Cisco Umbrella stara się zapewnić najlepszy z możliwych dostęp do Internetu każdemu z naszych ponad 85 milionów użytkowników. Naszą pasją jest opracowywanie nowych technologii mających na celu zwiększenie bezpieczeństwa oraz szybkości działania Internetu.

Globalna sieć platformy Umbrella obsługuje ponad 120 miliardów zapytań DNS dziennie.



Oto 10 powodów, dla których warto przekierować swój serwer DNS do platformy Umbrella:

Większe bezpieczeństwo

Wysoce skalowalna, zautomatyzowana ochrona Infrastruktura chroniona przed atakami DDoS, infekowaniem pamięci podręcznej oraz fałszywymi odpowiedziami zmniejsza zagrożenie ze strony cyberataków.	Zapewniamy naszym klientom odpowiednią ochronę, opracowując i wdrażając najlepsze w swojej klasie praktyki dotyczące serwerów DNS. Polegają one między innymi na blokowaniu lub ograniczaniu zapytań o nietypowych rekordach, nadmiarowych duplikowanych zapytań, nadmiarowych rekordów DNS lub rekordów wysyłanych ze złośliwych klienckich adresów IP oraz zwiększaniu entropii zapytań o adres serwera nazw.
Ulepszony kod resolwera DNS Zwiększenie specjalizacji kodu radykalnie zmniejsza prawdopodobieństwo wykorzystania luk w porównaniu z protokołem BIND lub Microsoft DNS.	Serwery w sieci platformy Umbrella wykorzystują prywatną gałąź kodu źródłowego djbdns, dzięki czemu powiązane z nimi systemy są zawsze chronione przez niezbędne poprawki. W porównaniu z protokołem BIND lub Microsoft DNS platforma Umbrella nie jest podatna na ataki polegające na przykład na infekowaniu pamięci podręcznej DNS, które zostały zaobserwowane w lipcu 2008 r.
Pierwsza usługa szyfrująca ruch na serwerach DNS Zabezpieczanie „ostatniego odcinka” ruchu DNS między użytkownikiem i dostawcą usług internetowych blokuje podsłuchiwanie i inne typy ataków.	Podobnie jak rozwiązanie SSL zamienia ruch w sieci WWW z realizowanego przy użyciu protokołu HTTP na realizowany przy użyciu protokołu HTTPS, platforma Umbrella używa funkcji DNSCrypt do szyfrowania ruchu na serwerach DNS. Opcjonalne oprogramowanie punktów końcowych zabezpiecza serwer DNS przed atakami ze strony pośredników bez żadnych zmian w nazwach domen lub sposobach ich działania.

Wyjątkowa niezawodność

Przejrzystość i doskonałość operacyjna

Nasz pracujący z zaangażowaniem zespół inżynierów sieciowych i ekspertów w dziedzinie serwerów DNS, dostępny całą dobę, siedem dni w tygodniu, zapewnia ciągłość i pewność obsługi.

Centrum operacji sieciowych Umbrella dokładnie kontroluje cały ruch internetowy pod kątem problemów z routingiem, a także monitoruje naszą globalną infrastrukturę w kierunku różnych zdarzeń. Od 2006 r. udostępniamy nasz stan systemu publicznie.

Routing w technologii anycast zmniejsza obciążenia administratorów

Obsługa wszystkich zapytań DNS przy użyciu tego samego adresu IP eliminuje złożoność sieci.

Platforma Umbrella ogłasza jeden adres IP dla setek resolwerów DNS we wszystkich lokalizacjach centrów danych. Nawet w przypadku przejścia wielu lokalizacji w tryb offline działanie usługi nie zostanie zakłócone, ponieważ zapytania DNS będą w przejrzysty sposób przekierowywane do kolejnej optymalnej lokalizacji. Dzięki temu zawsze dotrzesz tam, dokąd chcesz.

Inteligentniejsza technologia pamięci podręcznej DNS

Zastępowanie nieprawidłowych odpowiedzi ostatnim znanym adresem IP usprawnia korzystanie z Internetu.

Jeśli autorytatywny serwer nazw domeny stanie się niedostępny lub będzie nieprawidłowo skonfigurowany, wówczas funkcja SmartCache platformy Umbrella zwróci wygasłą odpowiedź DNS zamiast błędu. Gdy pozostali użytkownicy nie będą w stanie wyświetlić strony, Ty połączysz się z nią bez problemu.

Prędkość działania

Jedna z największych na świecie pamięci podręcznych DNS

Zna niemal każdą odpowiedź na potencjalne pytania, co pozwala zmniejszyć opóźnienia autorytatywnych serwerów nazw.

Wiemy, że nie możesz przez cały dzień oczekiwać na odpowiedź serwera DSN, dlatego też centra danych platformy Umbrella udostępniają odpowiedzi na wcześniejsze zapytania w ramach jednej globalnej pamięci podręcznej. Pozwala to uniknąć opóźnień związanych z oczekiwaniem na odpowiedź wielu autorytatywnych serwerów nazw na zapytanie DNS.

Ponad 500 równorzędnych usługodawców w punktach wymiany ruchu internetowego

Odpowiednie przekierowywanie zapytań i odpowiedzi przy zachowaniu minimalnej liczby punktów pośrednich skraca czas od wysłania zapytania do otrzymania odpowiedzi.

Platforma Umbrella korzysta ze wsparcia zaufanych usługodawców. Wymieniając trasy i ustanawiając wzajemne połączenia z ponad 500 największymi dostawcami usług internetowych i sieci na całym świecie, skracamy ścieżkę między Tobą i platformą Umbrella, a także między platformą Umbrella i autorytatywnymi serwerami nazw.

Integracja z sieciami CDN

Kierowanie sieci i urządzeń do łączenia się z najbliższą dostępną treścią ogranicza opóźnienia połączeń.

Platforma Umbrella, czołowe globalne sieci CDN i inni publiczni dostawcy usług DNS współpracują na rzecz przyspieszenia działania Internetu, umożliwiając sieciom CDN wysyłanie w odpowiedzi na zapytania DNS adresów IP najbliższych serwerów zawierających żądaną treść. Zmniejsza to opóźnienia wszelkich działań – od korzystania z kluczowych aplikacji biznesowych do przesyłania strumieniowego wideo.

Nadmiarowa i odporna infrastruktura

Skuteczne unieszkodliwianie zalewu złośliwych zapytań bez negatywnych skutków dla prawidłowych zapytań pozwala uniknąć spowolnień.

Jest to głównie kwestia bezpieczeństwa, jednak minimalizowanie skutków ataków niesie ze sobą również istotne korzyści dla wydajności sieci. Platforma Umbrella korzysta z nadmiarowych zasobów systemowych dla każdego rekurencyjnego resolwera w każdym centrum danych. Dzięki temu zapewnia przepustowość większą o rząd wielkości od przepustowości docelowej.

Wgląd w zabezpieczenia i kontrola nad nimi

Sprawdź, co się dzieje w Twoich sieciach

Cała aktywność w Internecie jest rejestrowana w czasie rzeczywistym i klasyfikowana według 8 rodzajów zagrożeń dla bezpieczeństwa oraz 80 rodzajów zawartości internetowej.

Musisz jedynie wprowadzić adresy IP Twoich sieci w naszym łatwym w obsłudze interfejsie internetowym, a następnie wyszukać, odfiltrować i wyeksportować dane dotyczące globalnej aktywności internetowej lub według sieci z ostatnich 30 dni.