Metody zabezpieczenia zasobów sieciowych w Windows Serwer.

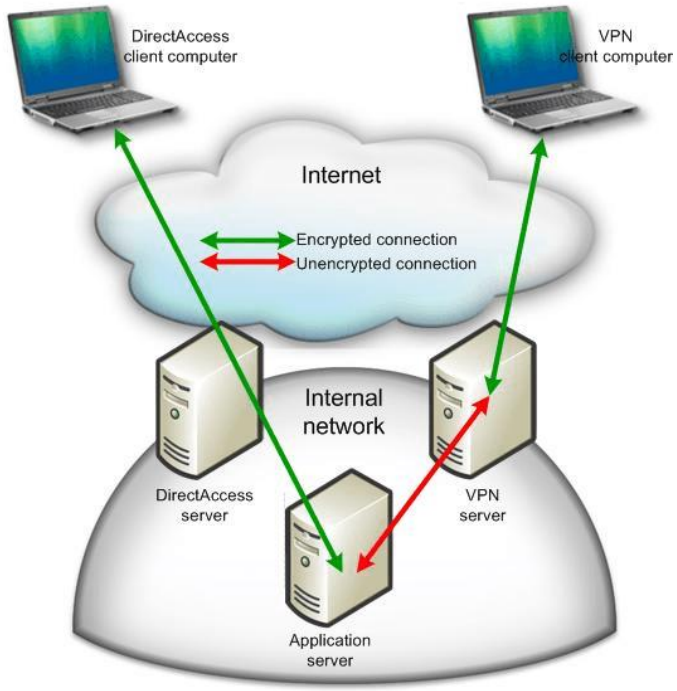
Omówienie Microsoft DirectAccess

W systemie Windows Server 2016 ochrona dostępu do sieci (NAP) została wycofana z systemu, co można zrobić, aby sprawdzić, czy klient VPN ma włączony Windows FireWall lub czy klient VPN ma najnowsze aktualizacje, wszystkie te funkcje były w ramach ochrony dostępu do sieci (NAP),
Jedyną rzeczą, która zbliża się do NAP, są zasady MDM i dostęp warunkowy oparty na zgodności za pośrednictwem usługi Intune/Azure AD, ale obejmuje tylko określone przypadki użycia i jest silnie uzależniony od platformy Azure.
NAP nie jest już technologią, w którą wierzy MS. Od 2012 roku ma status „przestarzałej".
Coraz więcej osób łączy się z siecią biurową z domu, jak możesz utrzymać ich produktywność bez narażania siebie i innych w sieci na potencjalne ryzyko?
Zdalne połączenie z organizacją to kolejna przeszkoda, z którą muszą zmierzyć się specjaliści IT.
Istnieją sposoby na przezwyciężenie potencjalnych zagrożeń bezpieczeństwa, zapewniając solidny dostęp zdalny. Wirtualne sieci prywatne (VPN) to tradycyjne rozwiązanie, z którego wielu z powodzeniem korzysta.

Microsoft DirectAccess.

Niektórzy specjaliści IT, uważają, że DirectAccess to tylko kolejne zaawansowane rozwiązanie VPN. Istnieje kilka podobieństw między VPN a DirectAccess, są one całkowicie różne pod względem podstawowej technologii i funkcjonalności.

Co to jest DirectAccess?



DirectAccess, znany również jako Unified Remote Access, to produkt firmy Microsoft zaprojektowany specjalnie dla systemu Windows. Został on początkowo wprowadzony w Windows Server 2008 i Windows 7 Enterprise Edition, aby umożliwić użytkownikom zdalny dostęp do zasobów sieci prywatnej za pomocą Internetu. DirectAccess to bezpieczniejsza, wygodniejsza i bardziej zaawansowana alternatywa niż tradycyjna sieć VPN.

DirectAccess ma przede wszystkim na celu zapewnienie użytkownikom płynnej łączności intranetowej. Oferuje przezroczyste, zawsze aktywne połączenie ustanowione przez maszynę, a nie przez użytkownika. Dlatego DirectAccess zaczyna zabezpieczać kanał sieciowy, gdy tylko klient uzyska aktywne połączenie internetowe. DirectAccess zapewnia także uwierzytelnione, bezpieczne i dwukierunkowe połączenie, zapewniając zdalny dostęp do użytkowników.

Co sprawia, że DirectAccess jest lepszy od VPN?

DirectAccess eliminuje niektóre poważne wady wdrażania VPN. Jak wspomniano wcześniej, połączenia VPN są inicjowane przez użytkownika, podczas gdy w przypadku DirectAccess połączenie jest inicjowane przez komputer. Ponadto wszyscy klienci są bezpośrednio połączeni z serwerami zarządzania, co zapewnia zgodność konfiguracji zabezpieczeń.

Połączenia DirectAccess są znacznie bezpieczniejsze niż te oferowane przez VPN, ponieważ wszyscy klienci DirectAccess muszą mieć certyfikat wydany przez samą organizację.

DirectAccess to funkcja przyjazna dla zapory ogniowej i nie jest ograniczona do żadnego obszaru geograficznego. Działa wszędzie, pod warunkiem, że użytkownik jest podłączony do Internetu.

I odwrotnie, sieci VPN napotykają przeszkody próbujące poradzić sobie z niektórymi zaporami ogniowymi i czasami mogą nie zapewnić bezpiecznego zdalnego dostępu do wszystkich lokalizacji.

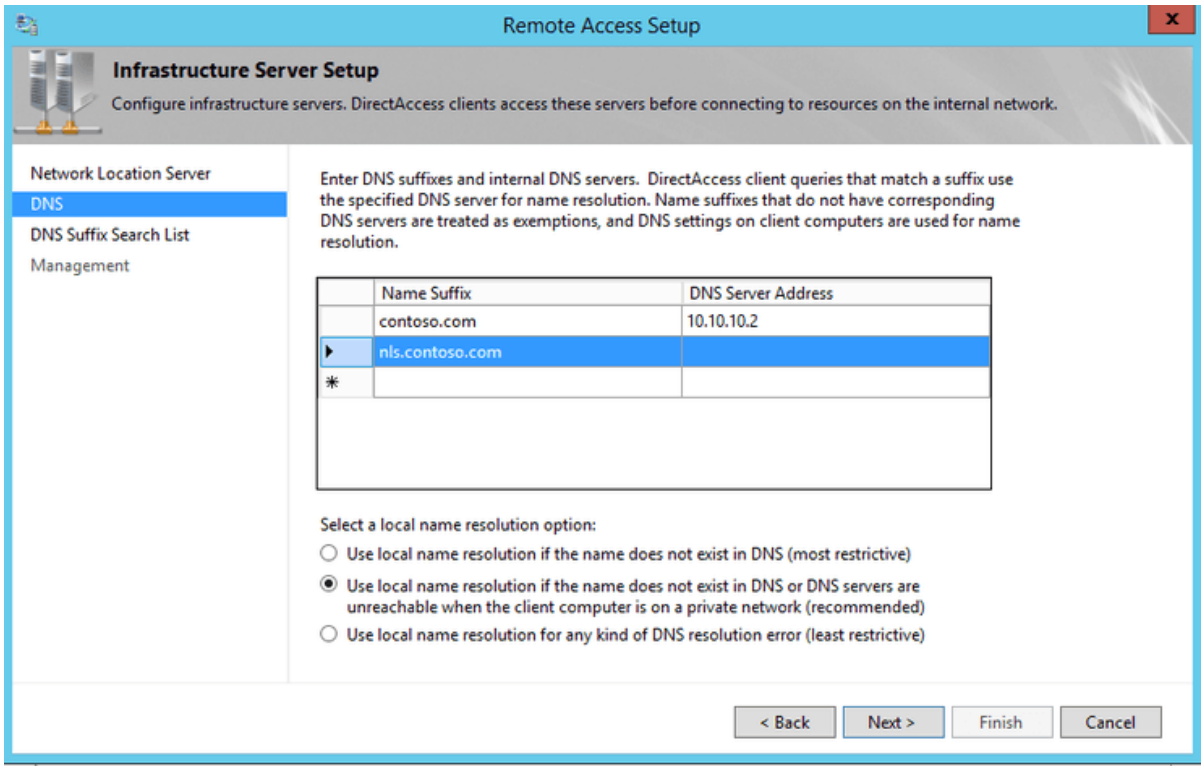
W DirectAccess wszyscy klienci są stale monitorowani i zarządzani przez serwer hosta lub serwer zarządzania, co minimalizuje zagrożenie intruzów w sieci.

W przypadku sieci VPN klient może wejść do sieci bez wiedzy o scentralizowanym serwerze, co może prowadzić do problemu bezpieczeństwa ze znacznym ryzykiem.

DirectAccess to połączenie dwukierunkowe. Dlatego wszystkie systemy klienckie w sieci DirectAccess są zawsze obsługiwane przez serwer zarządzania.

Serwer w sieci DirectAccess może łatwo rozwiązać problem w systemie klienta, co nie zawsze jest możliwe w sieci VPN.

VPN obejmuje złożony proces nawiązywania połączenia z siecią, co zmniejsza wydajność i wydajność pracowników. Z drugiej strony DirectAccess jest stosunkowo łatwy i bezproblemowy w konfiguracji, podłączeniu i użyciu.



Wymagania

Jeden kontroler domeny z systemem Windows Server 2003 lub nowszym.

Wewnętrzna infrastruktura PKI (Public Key Infrastructure) zaprojektowana przez organizację w celu przypisywania certyfikatów maszyn do klientów i serwerów.

Serwer DirectAccess musi działać w systemie Windows Server 2008 R2, a zarówno klienci, jak i serwer muszą działać w systemie Windows 7 Enterprise / Ultimate lub nowszym.

IPv6 musi być włączony na wszystkich klientach i serwerach, ponieważ jest to podstawa funkcjonowania DirectAccess.

Wszyscy klienci DirectAccess muszą należeć do domeny Active Directory.

Serwer DirectAccess musi mieć dwa adaptery interfejsu sieciowego do obsługi komunikacji dwukierunkowej.

Zalety DirectAccess

Zwiększone bezpieczeństwo

DirectAccess zapewnia w pełni szyfrowany i uwierzytelniony tryb połączenia.
Zapewnia pracownikom uwierzytelnione szyfrowanie IPSec w celu zapewnienia integralności i poufności. IPv6 jest podstawą wszystkich połączeń DirectAccess, wykorzystuje IPv6 do transportu.
Protokół IPv6 jest wdrażany, zapewniając pełną kompatybilność ze wszystkimi hostami IPv4.
DirectAccess jest zabezpieczony na kilku etapach w całym procesie zdalnego połączenia.
Wykorzystuje różne cyfrowe certyfikaty, standardy Kerberos i NTLM, aby utrzymać niezawodne, bezpieczne i uwierzytelnione połączenie.
Oprócz wszystkich wyżej wymienionych wbudowanych mechanizmów bezpieczeństwa w DirectAccess, organizacje mogą również integrować karty inteligentne i dynamiczne hasła jednorazowe w celu dodatkowego zabezpieczenia i zapewnienia, że tylko autoryzowani użytkownicy mogą łączyć się z organizacją.

Doświadczenie użytkownika

Ponieważ DirectAccess jest domyślnie dostarczany z zawsze aktywnym połączeniem, nie wymaga żadnej konkretnej akcji ani konfiguracji ze strony użytkownika, aby ustanowić zdalne połączenie.
DirectAccess zapewnia bezproblemową obsługę i pozwala użytkownikowi na zdalny dostęp do zasobów organizacyjnych w taki sam sposób, jak robią to z biura.

Niższe koszty pomocy technicznej i łatwość użytkowania

DirectAccess bezsprzecznie zapewnia lepszą obsługę użytkowników za pośrednictwem VPN lub dowolnego innego rozwiązania do zdalnej łączności.
W DirectAccess całe połączenie dostępu zdalnego jest ustanawiane na poziomie komputera, uwalniając użytkowników końcowych od długiego procesu nawiązywania połączenia zdalnego.
Ponieważ większość procesu połączenia zarządzana jest na poziomie komputera, wydajność użytkowników wzrasta.
Praca personelu wsparcia IT jest zmniejszona.

Obsługa równoważenia obciążenia

DirectAccess jest zintegrowany z rozwiązaniami równoważącymi obciążenie, aby zapewnić większą skalowalność i dostępność.

Wykorzystuje techniki równoważenia obciążenia sieciowego systemu Windows lub sprzętowy moduł równoważenia obciążenia pracowników, co pozwala użytkownikowi skonfigurować wiele serwerów DirectAccess w organizacji, aby obciążenie było równomiernie zrównoważone na wielu serwerach.

DirectAccess udowadnia, że mobilność nie jest już nie do pokonania w branży IT, dlatego jest wyborem wielu osób i organizacji.

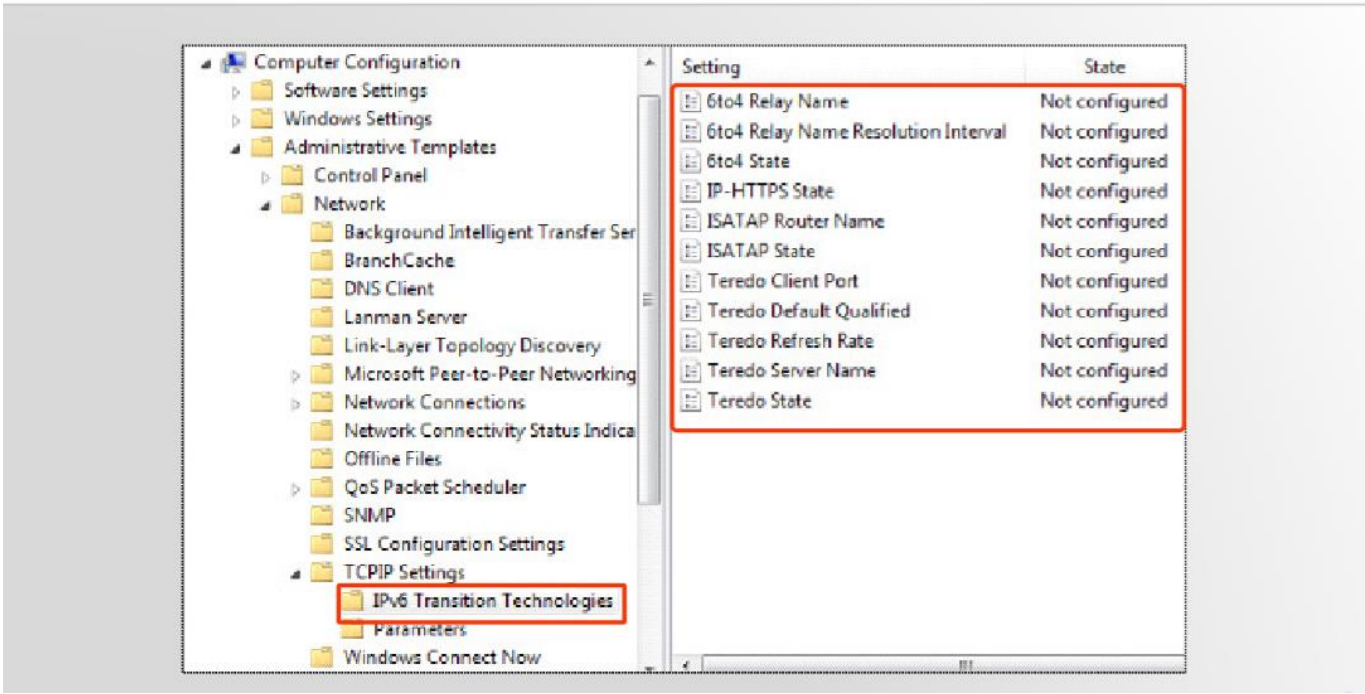
Metody połączeń DirectAccess

Połączenie klienta	Metoda połączenia DirectAccess
Adresacja publiczna IPv6	Adresacja publiczna IPv6
Adresacja publiczna IPv4	6to4
Adresacja prywatna IPv4 (NAT)	Teredo
Klient podłączony do sieci Internet ale bez możliwości połączenia do sieci z uwagi na ograniczenia np. ustawienia zapory ogniowej	IP-HTTPS

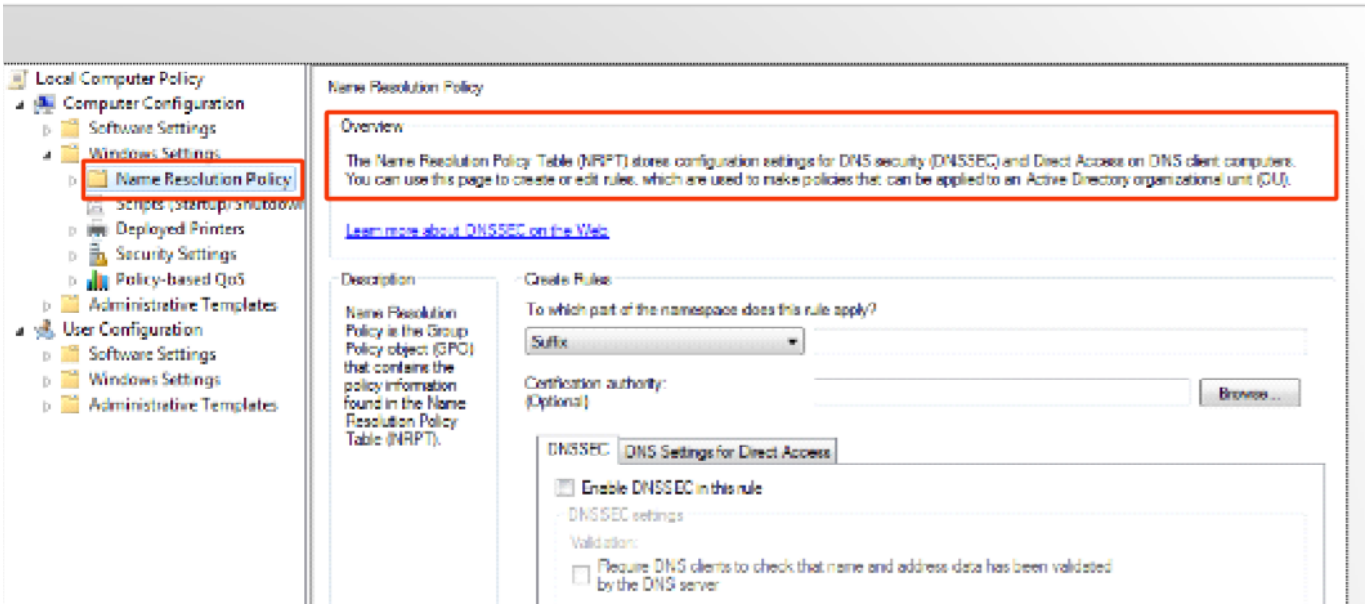
Konfiguracja klienta DirectAccess

- DirectAccess wspierany jest wyłączenie w ramach Windows 7 Ultimate i Enterprise dołączonych do domeny
- Konfiguracja DirectAccess wymaga dodania kont komputerów do specjalnej grupy zabezpieczeń
- Konfiguracja klienta DirectAccess realizowana jest przez Group Policy
- Działanie DirectAccess wymaga posiadania przez klienta certyfikatu dla komputera

Polityki konfiguracji klienta DirectAccess (1)



Polityki konfiguracji klienta DirectAccess (2)



Konfiguracja serwera DirectAccess

Zainstalowany Windows Server 2008 R2 będący członkiem domeny

Dwa interfejsy sieciowe

Ważny certyfikat na potrzeby uwierzytelniania serwera

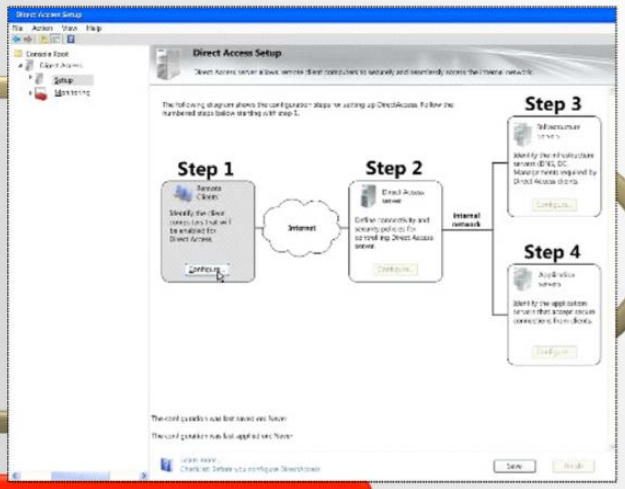
(1)
Połączenie z Internetem i przypisane do interfejsu dwa następujące po sobie adresy publiczne IPv4

(2)
Bezpośrednie połączenie z siecią korporacyjną

Utworzona globalna grupa zabezpieczeń (nazwa dowolna)

Konfiguracja serwera DirectAccess

DirectAccess Management Console



Ważne porty

UDP port 3544 >>> ruch Teredo
IPv4 protocol 41 >>> ruch 6to4
TCP port 443 >>> ruch IP-HTTPS
ICMPv6 and IPv4 Protocol 50 >>> klienci zdalni posiadający adresy IPv6

Źródła:

docs.microsoft.com

wss.pl