KORZYSTANIE Z 802.1X I MECHANIZMÓW KONTROLI DOSTĘPU DO SIECI — TRZY PROBLEMY DO UNIKNIĘCIA

OPRACOWANIE



STRESZCZENIE

Aby umożliwić kontrolę nad dostępem do sieci, architekci zabezpieczeń zazwyczaj korzystają ze standardu 802.1X lub komercyjnych mechanizmów kontroli dostępu do sieci (NAC). W kontekście bezpieczeństwa każda z tych opcji ma jednak pewne ograniczenia, zwłaszcza w obliczu szybkiego rozwoju sieci wynikającego z korzystania z urządzeń prywatnych do celów służbowych (BYOD) i urządzeń związanych z Internetem rzeczy (IoT). W niniejszym opracowaniu zaprezentowano ograniczenia każdego podejścia i przedstawiono trzy główne problemy do uniknięcia podczas projektowania mechanizmów kontroli dostępu do sieci: brak widoczności, brak kontroli i brak automatyzacji.



IDENTYFIKACJA ZAGROŻEŃ

Kto i co jest w sieci przedsiębiorstwa? W epoce połączeń przewodowych i urządzeń wyłącznie służbowych można było odpowiedzieć na te pytania znacznie łatwiej. Obecnie zdefiniowane i wyraźnie wyznaczone granice sieci praktycznie zniknęły. Pracownicy, partnerzy i goście chcą mieć bezprzewodowy dostęp zdalny do zasobów przedsiębiorstwa. Ponad połowa przedsiębiorstw akceptuje korzystanie z urządzeń prywatnych do celów służbowych[1]. Jednocześnie codziennie do sieci podłączany jest kolejny milion urządzeń związanych z Internetem rzeczy takich jak czujniki temperatury i mechanizmy sterujące budynkami[2].

W rezultacie dostęp do sieci jest trudniejszy do ochrony niż kiedykolwiek wcześniej, a wszystko to ma miejsce w kontekście znacznie większego narażenia na ryzyko ataków. W badaniach przeprowadzonych w 2018 r. przez Instytut SANS 42% respondentów stwierdziło, że w ciągu ostatniego roku bezpieczeństwo ich urządzeń końcowych zostało naruszone, a 20% respondentów przyznało, że nie wie, czy do takiego naruszenia doszło[3]. Urządzenia końcowe sieci to najczęstsze cele cyberataków. Ponadto przewiduje się, że do 2020 r. 25% wszystkich ataków będzie dotyczyć urządzeń związanych z Internetem rzeczy[4].

Architekci zabezpieczeń zazwyczaj stosują dwa podejścia do zabezpieczania dostępu do sieci. W przypadku pierwszego korzystają z utworzonego w 2001 r. standardu 802.1X służącego do uwierzytelniania użytkowników i urządzeń mających nawiązać połączenie z siecią. Jest to podstawowy element każdego kompleksowego mechanizmu kontroli dostępu do sieci. Sam w sobie nie jest to jednak kompleksowy mechanizm kontroli dostępu do sieci, ponieważ ma on szereg ograniczeń, które zostaną określone poniżej.

Drugie podejście polega na zastosowaniu mechanizmu kontroli dostępu do sieci (NAC). Pierwsze takie mechanizmy pojawiły się na rynku kilka lat po opublikowaniu standardu 802.1X. Pierwsza generacja tych mechanizmów uwierzytelniała urządzenia końcowe (głównie sprawdzone przez dział IT komputery PC) za pomocą prostej technologii typu „skanuj i blokuj". Druga generacja tych mechanizmów pozwalała również na zarządzanie dostępem do sieci gości. W niniejszym dokumencie porównano funkcje mechanizmów kontroli dostępu do sieci ze standardem 802.1X i określono trzy największe problemy do uniknięcia podczas projektowania tych mechanizmów.



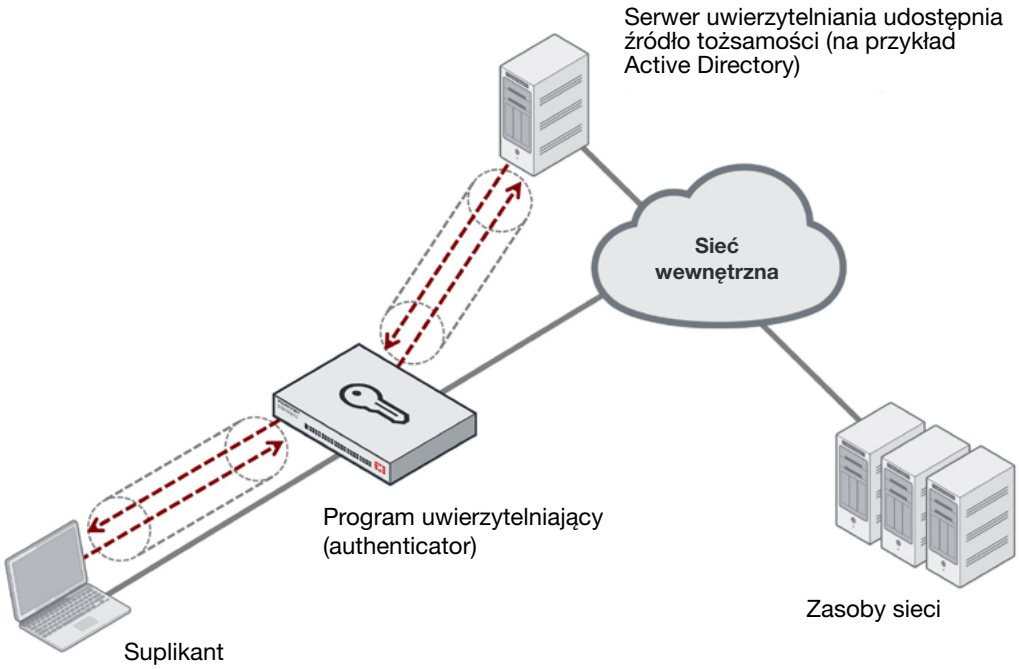
1 milion urządzeń związanych z Internetem rzeczy jest codziennie podłączanych do sieci.

42% respondentów zgłosiło w ubiegłym roku przypadki naruszenia bezpieczeństwa za pośrednictwem urządzeń końcowych.

1) BRAK WIDOCZNOŚCI — CO JEST W SIECI PRZEDSIĘBIORSTWA?

Nie można zabezpieczyć tego, czego nie widać w sieci. Standard 802.1X może pełnić funkcję strażnika dostępu zarówno do sieci przewodowych, jak i bezprzewodowych, nie zapewnia jednak wystarczającej widoczności i ochrony. Na rys. 1 przedstawiono ogólny schemat działania standardu 802.1X.

Ogólny zarys standardu 802.1X



RYS 1. W STANDARDZIE 802.1X PROGRAM UWIERZYTELNIAJĄCY WERYFIKUJE NAZWĘ UŻYTKOWNIKA I HASŁO SUPLIKANTA POD KĄTEM ZGODNOŚCI Z DANYMI ZAPISANYMI NA SERWERZE UWIERZYTELNIAJĄCYM (NA PRZYKŁAD W USŁUDZE ACTIVE DIRECTORY), ZANIM ZEZWOLI SUPLIKANTOWI NA DOSTĘP DO SIECI WEWNĘTRZNEJ.

Aby użyć prostej analogii, suplikant (supplicant) w standardzie 802.1X to gość czekający na wejście do klubu nocnego. Program uwierzytelniający (authenticator) pełni funkcję bramkarza i sprawdza dane identyfikacyjne gościa na liście zatwierdzonej przez kierownika klubu (serwer uwierzytelniania), zanim pozwoli gościowi wejść do środka. Po uwierzytelnieniu suplikant zostaje podłączony do sieci i na tym rola standardu 802.1X zasadniczo się kończy.

Mechanizmy kontroli dostępu do sieci (NAC) zapewniają natomiast funkcje bezpieczeństwa, których brakuje w standardzie 802.1X. Nie tylko bowiem uwierzytelniają urządzenie, ale także skanują je pod kątem zagrożeń i sprawdzają, czy jest zgodne z zasadami bezpieczeństwa, zanim zostanie podłączone do sieci. Niektóre mechanizmy kontroli dostępu dokonują uwierzytelniania bez używania standardu 802.1X, niektóre natomiast z nim współpracują, na przykład serwer RADIUS (Remote Authentication Dial-In User Service).

Nie istnieje żadna standardowa ani uzgodniona architektura mechanizmów kontroli dostępu do sieci. Niektóre mechanizmy nie zapewniają na przykład kompleksowej widoczności i inkluzywności potrzebnych w przypadku szybko rozwijających się sieci przedsiębiorstw. Poniżej przedstawiono luki w zabezpieczeniach tych mechanizmów oraz dodatkowe obawy dotyczące ochrony zapewnianej przez standard 802.1X.

KORZYSTANIE Z URZĄDZEŃ PRYWATNYCH DO CELÓW SŁUŻBOWYCH (BYOD)

Korzystanie z urządzeń prywatnych do celów służbowych jest coraz częstsze: podejście to stosuje już 87% przedsiębiorstw (w 2015 r. było to 74%)[5, 6]. Z badań wynika, że pracownicy korzystający z własnych urządzeń są bardziej produktywni, dzięki czemu mogą zaoszczędzić 58 minut dziennie[7]. Podejście to stanowi jednak poważne wyzwanie dla zespołów ds. bezpieczeństwa, które muszą znaleźć sposób na kontrolę i zabezpieczenie takich prywatnych urządzeń niesprawdzonych przez dział IT.

Podłączanie urządzeń do sieci za pomocą standardu 802.1X może sprawiać różnego rodzaju problemy:

- Każdy ośrodek musi mieć dostęp do serwera uwierzytelniania połączonego z centralną bazą danych (na przykład usługą Active Directory), a obsługa tego procesu może stanowić istotne obciążenie dla działu IT.
- Jeśli użytkownicy mogą podłączyć swoje urządzenia do sieci za pomocą jedynie nazw użytkownika i haseł, staje się to źródłem nieakceptowalnego ryzyka.
- Użytkownicy muszą zainstalować na swoich urządzeniach suplikant 802.1X, co może być dla nich trudne. Działanie takie poprawia proces uwierzytelniania, wymaga jednak większej pomocy ze strony działu IT.
- Mechanizmy kontroli dostępu z różnym skutkiem automatyzują proces podłączania do sieci przedsiębiorstwa urządzeń prywatnych.



URZĄDZENIA ZWIĄZANE Z INTERNETEM RZECZY

Liczba podłączonych do sieci urządzeń związanych z Internetem rzeczy, takich jak kamery bezpieczeństwa, rejestratory, czujniki temperatury i systemy kontroli oświetlenia, szybko rośnie. Wiele z tych urządzeń nie może wystąpić w roli suplikanta, nie może zatem korzystać z uwierzytelnienia 802.1X.

Pierwszą z dostępnych opcji jest odmowa im dostępu do sieci, ale nie jest to podejście realistyczne. Drugą opcją jest umieszczenie ich na białej liście (lista zatwierdzonych urządzeń), ale jest to działanie zasobochłonne i niebezpieczne. Trzecią opcją jest zarejestrowanie ich adresów MAC i ograniczenie do nich dostępu do sieci. Jest to działanie zasobochłonne i ryzykowne, ponieważ doświadczeni użytkownicy i hakerzy mogą sfałszować adresy MAC.

Niektóre mechanizmy kontroli dostępu do sieci mają swoje własne ograniczenia w kontekście zarządzania urządzeniami związanymi z Internetem rzeczy. Na przykład niektóre mechanizmy wymagają zainstalowania na urządzeniach agentów na potrzeby skanowania tych urządzeń, co stanowi problem, ponieważ na wielu z tych urządzeń nie można takiej instalacji dokonać.

GOŚCIE I PARTNERZY

Rozwiązania 802.1X mogą odpowiednio przypisać osoby niebędące pracownikami, takie jak goście, partnerzy lub wykonawcy, do wirtualnych sieci lokalnych (VLAN), aby umożliwić im dostęp do sieci WWW, ale ograniczyć lub uniemożliwić im dostęp do zasobów przedsiębiorstwa. W przypadku użytkowników korzystających z urządzeń prywatnych do celów służbowych pojawia się jednak zwiększone ryzyko dopuszczenia do sieci urządzeń niesprawdzonych przez dział IT i nieprzeskanowanych. Wymóg instalacji oprogramowania suplikanckiego na takich urządzeniach przyczynia się do poprawy możliwości uwierzytelnienia, ale zwiększa również wymagania wobec użytkowników oraz działu IT.

PRZEWODOWE SIECI LOKALNE

Korzystanie z przewodowych sieci lokalnych wiąże się z szeregiem problemów, które sprawiają, że wdrożenie strategii 802.1X jest złożone i kosztowne. Wiele starszych urządzeń końcowych i niektóre starsze przełączniki nie obsługują oprogramowania suplikanckiego w standardzie 802.1X. Ponadto inne przełączniki od różnych dostawców obsługują standard 802.1X w różny sposób. Dodatkowo konfiguracja przełącznika obsługującego kombinację urządzeń końcowych 802.1X i innych niż 802.1X jest trudna i zasobochłonna, co może ograniczyć widoczność sieci i zwiększyć jej narażenie na ryzyko.

Niezależnie zatem od tego, czy zarządza się przewodową, czy bezprzewodową siecią lokalną, ograniczenia standardu 802.1X lub mechanizmów kontroli dostępu pierwszej i drugiej generacji utrudniają lub uniemożliwiają uzyskanie pełnej widoczności użytkowników i urządzeń w sieci przedsiębiorstwa.



Pracownicy korzystający z urządzeń prywatnych do celów służbowych oszczędzają

58 minut dziennie.

WYZWANIA ZWIĄZANE Z ZAPEWNIENIEM WIDOCZNOŚCI

Potrzeba	802.1X	NAC
Uwierzytelnienie nazwy użytkownika i hasła	X	X
Uwierzytelnienie urządzenia	O ile zainstalowano oprogramowanie suplikanckie	X
Automatyczne podłączanie do sieci w modelu BYOD	Złożone — może wymagać pomocy działu IT	Zróżnicowane — może wymagać oprogramowania agenta
Obsługa Internetu rzeczy	Większość urządzeń związanych z Internetem rzeczy nie obsługuje oprogramowania suplikanckiego	Zróżnicowane — może wymagać oprogramowania agenta
Wirtualne sieci lokalne gości i partnerów	O ile zainstalowano oprogramowanie suplikanckie	X
Przewodowe sieci lokalne	Problemy i wyjątki	X



2) BRAK KONTROLI — JAK ZMINIMALIZOWAĆ RYZYKO?

Rozwiązania 802.1X mogą uwierzytelniać użytkownika i urządzenie, ale nie skanują takiego urządzenia w celu oceny i poprawy jego stanu bezpieczeństwa przed udzieleniem mu dostępu do sieci. Można to porównać z sytuacją, gdy agent ochrony lotniska sprawdza dokumenty pasażerów i wpuszcza ich na pokład samolotu, ale nie przeszukuje ich bagażu w poszukiwaniu zagrożeń.

Dlaczego jest to ważne? 63% przedsiębiorstw nie monitoruje urządzeń końcowych po ich odłączeniu od sieci, a następnie ponownym podłączeniu[8], mimo że w tym czasie mogły zostać zaatakowane. Jednocześnie średni koszt naruszenia bezpieczeństwa za pośrednictwem jednego urządzenia końcowego wyniósł w 2017 r. już 5 mln USD[9].

Zezwolenie urządzeniu na dostęp do sieci bez jego przeskanowania jest oczywiście nierozsądne. Ponadto w modelu 802.1X urządzenia nie są monitorowane **po** podłączeniu ich do sieci. W modelu takim nie można zatem:

- Wykrywać ani blokować zaatakowanych urządzeń w sieci ani blokować dostępu do sieci, gdy takie urządzenia zostaną wykryte.
- Ograniczać ruchu w sieci wewnętrznej (w drodze segmentacji sieci przez dynamiczne przypisywanie wirtualnych sieci lokalnych), jeśli naruszenie bezpieczeństwa zostanie wykryte **po udzieleniu dostępu do sieci** (standard 802.1X **może** być użyty tylko w celu przypisania wirtualnej sieci lokalnej **podczas** udzielania dostępu do sieci).
- Egzekwować szczegółowych zasad dostępu opartych na rolach po udzieleniu dostępu do sieci (na przykład kamera IP powinna mieć dostęp do serwera filmów, a nie do innych części sieci).
- Monitorować bieżącej zgodności z zasadami ani prowadzić dzienników logowania, raportowania i audytu na potrzeby lepszej kontroli zgodności.

Niektóre mechanizmy kontroli dostępu można łączyć z rozwiązaniami 802.1X na potrzeby skanowania urządzeń i weryfikacji ich stanu bezpieczeństwa przed podłączeniem ich do sieci. Jeśli dane urządzenie nie jest zgodne z zasadami bezpieczeństwa, wspomniane mechanizmy mogą podłączyć je do specjalnej wirtualnej sieci lokalnej, w ramach której dostęp jest ograniczony dopóty, dopóki to urządzenie będzie zgodne z określonymi zasadami (zostanie usunięte złośliwe oprogramowanie, zostaną zainstalowane odpowiednie poprawki itp.).

Ponadto niektóre mechanizmy kontroli dostępu do sieci mogą skanować urządzenia **po podłączeniu ich do sieci**, aby wykonać niektóre albo wszystkie wymienione powyżej funkcje. Zdolności tych mechanizmów są jednak różne: niektóre z nich wymagają zainstalowania na urządzeniach agentów lub oprogramowania klienckiego, aby umożliwić ich skanowanie po podłączeniu do sieci. Może to sprawić, że podłączenie do sieci urządzeń prywatnych używanych do celów służbowych lub urządzeń związanych z Internetem rzeczy będzie trudne lub niemożliwe.



63% przedsiębiorstw nie jest zdolnych do monitorowania urządzeń końcowych po odłączeniu ich od sieci.

WYZWANIA ZWIĄZANE Z ZAPEWNIENIEM KONTROLI

Potrzeba	802.1X	NAC
Skanowanie urządzenia pod kątem zagrożeń **przed** podłączeniem go do sieci	—	X
Skanowanie urządzenia **po** podłączeniu go do sieci w celu identyfikowania i blokowania zagrożeń	—	Zróżnicowane — może wymagać oprogramowania agenta
Ograniczenie ruchu w sieci wewnętrznej, przypisanie wirtualnej sieci lokalnej **przed** podłączeniem urządzenia do sieci	X	X
Egzekwowanie zasad dostępu **po** podłączeniu urządzenia do sieci	—	Zróżnicowane — może wymagać oprogramowania agenta
Prowadzenie dzienników logowania, raportowania i audytu	—	Zróżnicowane



3) BRAK AUTOMATYZACJI — NIEWYSTARCZAJĄCE ZASOBY, ABY PRZECIWDZIAŁAĆ ZAGROŻENIOM

Obecnie zespoły ds. bezpieczeństwa są zazwyczaj przeciążone pracą. Na całym świecie liczba wakatów związanych z bezpieczeństwem cybernetycznym przekroczyła milion, a w ciągu kilku lat może wzrosnąć do 3,5 mln[10]. Tymczasem codziennie zespoły te otrzymują tysiące alertów bezpieczeństwa, a wiele z tych zespołów nie dysponuje przepustowością pozwalającą na ręczne zajęcie się każdym potencjalnym zagrożeniem sieciowym. Rozwiązania 802.1X lub mechanizmy kontroli dostępu, które nie oferują zaawansowanych funkcji automatyzacji, nie są również zdolne do wykrycia i ograniczenia skutków wszystkich zagrożeń, przez co przedsiębiorstwo jest w jeszcze większym stopniu narażone na ryzyko naruszenia bezpieczeństwa sieci.

Niektóre mechanizmy kontroli dostępu mogą również znacznie obciążać zasoby kadrowe działów IT i zwiększać ryzyko naruszenia bezpieczeństwa sieci w przypadku braku integracji i interoperacyjności z innymi zabezpieczeniami. W szczególności, gdy mechanizmy kontroli dostępu wykrywają ukierunkowane, ryzykowne zachowanie, mogą nie być zdolne do:

- Przesłania informacji (m.in. danych identyfikujących użytkownika i informacji o stanie bezpieczeństwa i lokalizacji urządzenia) do innych rozwiązań zabezpieczających takich jak system wykrywania włamań (IDS), system ochrony przed włamaniami (IPS), system ochrony przed utratą danych (DLP) oraz system zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM).
- Zbierania informacji z systemu zarządzania użyciem urządzeń przenośnych w przedsiębiorstwie (EMM) w celu określenia, czy dane urządzenie należy do przedsiębiorstwa.
- Poddania się automatyzacji w celu inicjowania zmian w konfiguracji innych urządzeń i izolowania zagrożeń.

Już obciążone pracą zespoły ds. bezpieczeństwa stoją w obliczu znacznego dodatkowego ryzyka, jeśli stosowane przez nie mechanizmy kontroli dostępu nie mogą zostać zintegrowane z innymi zabezpieczeniami na potrzeby skoordynowanej i zautomatyzowanej reakcji na zagrożenia.

Na całym świecie jest ponad

1 mln

wakatów związanych z cyberbezpieczeństwem.

WYZWANIA ZWIĄZANE Z AUTOMATYZACJĄ

Potrzeba	802.1X	NAC
Przesyłanie informacji o zagrożeniach do innych zabezpieczeń	—	Zróżnicowane
Zbieranie danych z systemu EMM w celu sprawdzenia, czy dane urządzenie należy do przedsiębiorstwa	—	Zróżnicowane
Zapewnienie zautomatyzowanej i skoordynowanej z innymi zabezpieczeniami reakcji na ukierunkowane zachowanie	—	Zróżnicowane



W POSZUKIWANIU KONTROLI

Rozwiązania 802.1X same w sobie, a nawet w połączeniu z wieloma mechanizmami kontroli dostępu do sieci, nie są odpowiednie do ochrony rozwijających się sieci obejmujących urządzenia związane z Internetem rzeczy i urządzenia prywatne używane do celów służbowych oraz nowych wymagań dotyczących dostępu gości i partnerów. Także wspomniane mechanizmy kontroli dostępu do sieci nie oferują takich samych funkcji, ponieważ mają różne architektury i podejścia do uwierzytelniania.

Podczas oceny tych mechanizmów architekci zabezpieczeń muszą zatem szukać zaawansowanych rozwiązań trzeciej generacji, które:

- Wypełnią luki w zabezpieczeniach rozwiązań 802.1X
- Wyeliminują problemy wynikające z podłączania do sieci urządzeń prywatnych używanych do celów służbowych i urządzeń związanych z Internetem rzeczy
- Unikną problemów związanych z brakiem widoczności, kontroli i automatyzacji

[1] Josh Bouk, „Top BYOD Trends for 2018", Cass Information Systems, Inc., 14 listopada 2017 r.

[2] „25% Of Cyberattacks Will Target IoT In 2020", Retail TouchPoints, dostęp z dnia 6 września 2018 r.

[3] Lee Neely, „Endpoint Protection and Response: A SANS Survey", SANS Institute, 12 czerwca 2018 r.

[4] „25% Of Cyberattacks Will Target IoT In 2020", Retail TouchPoints, dostęp z dnia 6 września 2018 r.

[5] „BYOD Usage in the Enterprise", Syntonic, lato 2016 r.

[6] Teena Maddox, „Research: 74 percent using or adopting BYOD", ZDNet, 5 stycznia 2015 r.

[7] Melanie Turek, „Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research", Samsung Insights, 3 sierpnia 2016 r.

[8] „The Cost of Insecure Endpoints", Ponemon Institute, dostęp z dnia 1 listopada 2018 r.

[9] Charlie Osborne, „Fileless attacks surge in 2017, security solutions are not stopping them", ZDNet, 15 listopada 2017 r.

[10] Steve Morgan, „Cybersecurity Jobs Report 2018–2021", Cybersecurity Ventures, 31 maja 2017 r.

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

POLSKA
ul. Złota 59
Budynek Lumen II
(6 piętro)
00-120 Warszawa
Polska

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

CENTRALA — AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

Copyright © 2018 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

253941-0-1-PL

maja 21, 2019 9:58 AM

WP-Understanding-nac-PL-A4