SafeGuard | Network Access Control

I-BS.PL

Centrum zabezpieczeń, organizacji i kontroli dostępów sieci

SafeGuard porządkuje dostęp do sieci i zasobów organizacji — w centrali, oddziałach i podczas pracy zdalnej. System pozwala określić, kto uzyskuje dostęp, z jakiego urządzenia i do jakich obszarów infrastruktury.

Dostęp nie opiera się wyłącznie na lokalizacji, porcie czy adresie IP. SafeGuard wiąże go z tożsamością użytkownika, urządzeniem oraz zasadami organizacji, dzięki czemu reguły dostępu są spójne i łatwiejsze do utrzymania.

Model działania:

- użytkownik i urządzenie są identyfikowane w systemie,
- dostęp przypisywany jest do osoby i jej roli,
- ruch sieciowy podlega zdefiniowanym regułom,
- zmiany wymagają zatwierdzenia zgodnie z polityką organizacji,
- dostęp ograniczony jest do określonych zasobów i relacji komunikacyjnych.

SafeGuard współpracuje ze switchami zarządzalnymi oraz urządzeniami FortiGate, wspierając aktualne wersje ich systemu (FortiOS).

Ryzyka rozproszonego dostępu

Wraz ze zmianami w organizacji rośnie liczba użytkowników, urządzeń, lokalizacji i wyjątków, które trzeba utrzymać pod kontrolą. W praktyce oznacza to, że:

- decyzje o dostępie są rozproszone między różne miejsca i konfiguracje,
- wyjątki narastają wraz ze zmianami w organizacji,
- administratorzy tracą czas na sprawdzanie zależności,
- różne lokalizacje wymagają osobnej obsługi,
- pojedyncza zmiana w konfiguracji może mieć nieoczywisty wpływ na inne obszary sieci,
- historia decyzji bywa trudna do odtworzenia.

Co zmienia SafeGuard

SafeGuard pozwala oprzeć dostęp na wspólnym modelu działania, który obejmuje użytkowników, urządzenia, reguły i zmiany w sieci. Dzięki temu system:

- skupia decyzje dostępowe w jednym uporządkowanym modelu,
- ogranicza liczbę lokalnych wyjątków i obejść,
- ułatwia ocenę skutków zmian przed ich wdrożeniem,
- ujednolica zasady dla centrali, oddziałów i pracy zdalnej,
- pomaga utrzymać kontrolę nad dostępem w rozwijającej się sieci.
- ułatwia odtworzenie historii decyzji i zmian.

Kontrola dostępu oparta na tożsamości

Segmentacja komunikacji
Ruch w sieci ograniczany jest do określonych relacji między zasobami. Zmniejsza to zakres niepożądanej komunikacji i pomaga ograniczyć skutki potencjalnych incydentów.

Kontrola zmian
Zmiany w dostępie i konfiguracji mogą być weryfikowane przed wdrożeniem. Pomaga to ograniczyć błędy administracyjne, nieprzewidziane skutki operacyjne i naruszenia przyjętych zasad.

Tożsamość AD / MAC
Użytkownik i urządzenie są identyfikowani niezależnie od miejsca podłączenia. Uprawnienia są powiązane z tożsamością, a nie wyłącznie z adresem IP lub portem sieciowym.

Polityki dostępu
Dostęp wynika z ról, grup i reguł zdefiniowanych w systemie. Administrator może określić, do jakich zasobów użytkownik ma dostęp i w jakim zakresie.

SafeGuard | Network Access Control

Jeden model zarządzania dostępem do sieci

SafeGuard przenosi obsługę dostępów do jednego procesu: od zgłoszenia potrzeby, przez zatwierdzenie, po nadanie, ograniczenie lub wygaszenie uprawnień. Administratorzy mogą zarządzać użytkownikami, grupami, dostępem czasowym i gośćmi bez utrzymywania lokalnych wyjątków w wielu miejscach infrastruktury.

Każda decyzja pozostaje widoczna w systemie. Łatwiej sprawdzić, kto otrzymał dostęp, na jakiej podstawie i przez jaki czas może z niego korzystać.

Uprawnienia zgodne z polityką organizacji

SafeGuard pozwala nadawać dostęp zgodnie z ustalonymi zasadami: rolą użytkownika, przynależnością do grupy, harmonogramem, dostępem czasowym albo zaakceptowanym wnioskiem.
Administratorzy mogą szybciej sprawdzić, z czego wynika dane uprawnienie, kiedy zostało nadane i czy nadal odpowiada aktualnym potrzebom organizacji.

Cykl obsługi dostępu

01

Zgłoszenie potrzeby

Dostęp może wynikać z roli użytkownika, przynależności do grupy, harmonogramu, dostępu czasowego albo złożonego wniosku.

02

Weryfikacja zasad

System sprawdza, czy zgłoszony lub przypisywany dostęp mieści się w ustalonych regułach. W przypadku dostępu wymagającego akceptacji decyzja może zostać przekazana do administratora lub osoby zatwierdzającej.

03

Nadanie lub ograniczenie uprawnień

System przypisuje dostęp zgodnie z decyzją administratora. Uprawnienia mogą zostać nadane, zawężone, zmienione lub wygaszone po określonym czasie.

04

Rejestr działań

Informacje o wnioskach, zmianach i nadanych dostępach pozostają dostępne w systemie. Ułatwia to późniejszą analizę, kontrolę i odtworzenie historii decyzji.

Zarządzanie dostępem

Dostępy tymczasowe i harmonogramy
Uprawnienia mogą obowiązywać tylko w określonym czasie lub zgodnie z harmonogramem. Pomaga to ograniczyć dostęp po zakończeniu zadania, poza godzinami pracy albo po zmianie zakresu obowiązków.

Dostęp dla gości
System umożliwia nadawanie gościom ograniczonego dostępu do sieci. Obsługuje dostęp czasowy, samorejestrację oraz zarządzanie danymi zgodnie z wymaganiami RODO.

Wnioski dostępowe
Użytkownicy mogą składać wnioski o dostęp bezpośrednio w systemie. Administratorzy widzą zgłoszenie, jego status i decyzję bez prowadzenia obsługi poza głównym procesem.

Dostęp indywidualny i grupowy
Uprawnienia mogą być nadawane pojedynczym użytkownikom lub całym grupom. Ułatwia to obsługę większych środowisk i ogranicza ręczne odtwarzanie tych samych ustawień.

I-BS.PL

Sieć, którą można kontrolować

SafeGuard daje administratorom szerszy kontekst zmian w sieci: pokazuje adresację, strukturę VLAN, powiązania między zasobami i zależności konfiguracji. Dzięki temu decyzje techniczne można podejmować z uwzględnieniem wpływu na całe środowisko.

System ogranicza konieczność ręcznej analizy wielu miejsc infrastruktury i pomaga szybciej ocenić, które elementy sieci są ze sobą powiązane

Standardowe podejście a SafeGuard

Standardowe podejście często rozdziela dostęp, adresację i konfigurację między różne narzędzia. **SafeGuard** łączy je z widokiem zależności, zmian i operacji sieciowych.

Obszar	Standardowy NAC	SafeGuard
model dostępu	oparty głównie na porcie/VLAN	uwzględnia użytkownika, urządzenie i reguły dostępu
dostęp zdalny	często zarządzany osobno względem dostępu lokalnego	spójny dla różnych lokalizacji i trybów pracy
komunikacja w sieci	ograniczona na poziomie segmentów	definiowana jako relacje między zasobami
adresacja	zarządzana osobno, poza systemem kontroli dostępu	powiązana ze strukturą VLAN, dostępami i obsługą oddziałów
widoczność zależności	fragmentaryczna, zależna od wielu narzędzi	obejmuje powiązania między dostępami, urządzeniami i zasobami
zarządzanie	rozproszone, zależne od infrastruktury	prowadzone z jednego środowiska administracyjnego
zmiany konfiguracji	ręczne, wymagają wiedzy o zależnościach	weryfikowane automatycznie przed wdrożeniem
obsługa zmian	zależna od ręcznej analizy konfiguracji	wspierana przez kontrolę powiązań i proces akceptacji
operacje	czasochłonne, manualne	oparte na powtarzalnych schematach działania
praca administratora	wymaga przełączania się między narzędziami	wspierana przez interfejs webowy, wyszukiwanie, migracje i klonowanie dostępów

Struktura i operacje w sieci

Adresacja i IPAM
Centralne zarządzanie adresacją i strukturą VLAN ułatwia utrzymanie porządku w środowisku sieciowym. Pomaga obsługiwać wiele oddziałów, grup urządzeń i zależności między elementami infrastruktury.

Mapa zależności w sieci
System pokazuje powiązania między urządzeniami, zasobami i konfiguracją. Administrator może szybciej ocenić, na które elementy wpłynie planowana zmiana.

Automatyzacja operacji
Migracje użytkowników, klonowanie dostępów i zmiany konfiguracji mogą być realizowane według powtarzalnych schematów. Ogranicza to liczbę ręcznych operacji oraz ryzyko pominięcia zależności.

Weryfikacja konfiguracji
System sprawdza powiązania przed wprowadzeniem zmian. Pomaga wykryć błędy wcześniej i ogranicza ryzyko niezamierzonego wpływu jednej operacji na inne elementy sieci.

Spójne zasady w całej organizacji

SafeGuard pomaga utrzymać jednolity sposób zarządzania dostępem, adresacją i zmianami w środowisku sieciowym. Dzięki temu organizacja zyskuje większą przewidywalność działań administracyjnych.
System wspiera codzienną pracę IT przy reorganizacjach, rozwoju infrastruktury i obsłudze rozproszonych jednostek, ograniczając konieczność ręcznego odtwarzania konfiguracji.

Stały rozwój systemu
SafeGuard jest rozwijany wraz z potrzebami organizacji i wymaganiami środowisk sieciowych. Kolejne funkcje usprawniają pracę administratorów i wzmacniają kontrolę nad dostępem.

Wsparcie dla rozproszonych struktur
System wspiera wspólny model zarządzania dla centrali, oddziałów, użytkowników, urządzeń i reguł komunikacji.

Bezpieczne zmiany administracyjne
Mechanizmy zatwierdzania i weryfikacji ograniczają ryzyko przypadkowych zmian, błędnych konfiguracji oraz nieprzewidzianych skutków operacyjnych.

Szybsza analiza sytuacji
Administratorzy mogą szybciej sprawdzić stan dostępów, urządzeń i zależności w sieci. Skraca to analizę i ułatwia reakcję.

Decyzja o dostępie to decyzja o bezpieczeństwie sieci

SafeGuard pomaga utrzymać jednolite zasady zarządzania dostępem, adresacją i zmianami w całej organizacji. Dzięki temu działania administracyjne są bardziej przewidywalne i łatwiejsze do kontrolowania.

Najważniejsze korzyści dla organizacji:

- jedno centrum zarządzania dostępem i siecią,
- mniej incydentów i większa pewność działania,
- łatwiejsze utrzymanie rozproszonych jednostek,
- szybsze wdrożenia i zmiany w infrastrukturze,
- lepsza organizacja pracy administratorów,
- szybsze decyzje dzięki pełnemu wglądowi w sieć,
- większa gotowość na audyty i kontrole.

Korzyści biznesowe:

- niższe i bardziej przewidywalne koszty utrzymania,
- mniej ręcznych operacji po stronie zespołu IT,
- mniejsze ryzyko błędnych decyzji i kosztownych przestojów,
- szybsze wdrażanie nowych osób i reorganizacji,
- lepsze wykorzystanie zasobów IT,
- łatwiejsze skalowanie organizacji,
- większa przewidywalność codziennych operacji.

Poznaj pozostałe rozwiązania z rodziny Safe

SafeConnect

Dostęp uprzywilejowany pod pełną kontrolą.
www.i-bs.pl/safeconnect

SafeDR

Backup i odtworzenie środowiska w jednym systemie.
www.i-bs.pl/safedr

I-BS.PL

www.i-bs.pl/safeguard

Chcesz zobaczyć, jak SafeGuard porządkuje dostęp do sieci?
Skontaktuj się z nami — odpowiemy na pytania i przedstawimy szczegóły oferty.

Joanna Stępień
tel.: 788 679 946
j.stepien@i-bs.pl

Bartłomiej Skoczylas
tel.: 728 403 586
b.skoczylas@i-bs.pl