CISCO
SECURE

Cisco Secure Firewall

Integracja sieci i bezpieczeństwa

Światowej klasy mechanizmy kontroli zabezpieczeń

Spójne zasady i widoczność

Sieć jako rozszerzenie architektury zabezpieczeń

W miarę jak aplikacje biznesowe o znaczeniu krytycznym przenoszą się z sieci lokalnych do chmury, a użytkownicy uzyskują dostęp do zasobów z urządzeń osobistych, podejście oparte na tradycyjnych zabezpieczeniach przestaje być skuteczne.

Pojedyncza sieć obwodowa przekształciła się w liczne mikroobwody, a tradycyjne zapory otrzymały wsparcie w postaci zarówno urządzeń fizycznych, jak i wirtualnych. W rezultacie organizacje zmagają się z obsługą różnorodnych zabezpieczeń, a także utrzymaniem spójnych zasad i jednolitej widoczności zagrożeń.

Cisco tworzy platformę zabezpieczeń, która umożliwia bardziej elastyczne i zintegrowane podejście do harmonizacji zasad i ich egzekwowania w coraz bardziej niejednorodnych sieciach.

Secure Firewall oferuje najgłębszą integrację podstawowych funkcji sieciowych i ochrony, zapewniając najbezpieczniejszą na rynku architekturę. Efektem jest kompletne portfolio zabezpieczeń, które chronią aplikacje i użytkowników na całym świecie.

Historie klientów

Korzyści

- Wykorzystanie dotychczasowych inwestycji w rozwiązania Cisco
- Egzekwowanie zasad dzięki lepszym punktom kontroli zabezpieczeń
- Ochrona użytkowników wszędzie tam, gdzie mają dostęp do internetu
- Rozszerzenie możliwości urządzeń sieciowych w celu uzyskania lepszych, bardziej zintegrowanych zabezpieczeń
- Niezawodna integracja produktów

Dlaczego Cisco?

Oferta Cisco Secure Firewall zapewnia lepszą ochronę sieci przed wciąż zmieniającymi się, złożonymi zagrożeniami. To inwestycja w elastyczny, zintegrowany fundament zabezpieczeń – ochronę najlepszą dziś i w niedalekiej przyszłości.

Od centrum danych przez oddziały po środowiska chmurowe – moc Cisco przekształci istniejącą infrastrukturę sieciową w najwyższej klasy mechanizmy kontroli zabezpieczeń wszędzie tam, gdzie są potrzebne.

Secure Firewall to niezawodna ochrona przed nawet najbardziej wyrafinowanymi zagrożeniami, która nie obniża wydajności podczas kontroli zaszyfrowanego ruchu. A integracja z innymi rozwiązaniami Cisco zapewnia niezwykle szeroką gamę produktów zabezpieczających, współpracujących ze sobą w celu skorelowania niepołączonych ze sobą wcześniej zdarzeń, eliminacji zakłóceń i szybszego blokowania zagrożeń.

Światowej klasy mechanizmy kontroli zabezpieczeń

Zagrożenia stały się bardziej wyrafinowane, a sieci – bardziej złożone. Tylko nieliczne organizacje posiadają zasoby, które mogą przeznaczyć na bieżące i skuteczne przeciwdziałanie wciąż zmieniającym się zagrożeniom.

W miarę jak zwiększa się złożoność zarówno zagrożeń, jak i sieci, posiadanie odpowiednich narzędzi do ochrony danych, aplikacji i sieci to absolutna konieczność. Urządzenia Cisco Secure Firewall oferują moc i elastyczność, które pozwolą pozostać zawsze o krok przed zagrożeniami. Oferują spektakularny, 3-krotny wzrost wydajności w porównaniu z urządzeniami poprzedniej generacji, jak również wyjątkowe możliwości sprzętowe do kontroli zaszyfrowanego ruchu na dużą skalę. Z kolei integracja z Cisco Secure Workload umożliwia dynamiczny wgląd w aplikacje i kontrolę nad nimi, co przekłada się na spójną ochronę nowoczesnych rozwiązań w całej sieci i przy dużym obciążeniu.

Historie klientów | Demo

Spójne zasady i widoczność

Oferta Secure Firewall to wyższy poziom zabezpieczeń wraz z przyszłościowym, elastycznym zarządzaniem. W zależności od potrzeb technologicznych i biznesowych Cisco oferuje różnorodne opcje zarządzania, w tym: Firewall Device Manager (FDM), Cisco Secure Firewall Management Center (FMC), Cisco Defense Orchestrator (CDO) i Cisco Security Analytics and Logging.

Cisco FDM to rozwiązanie do lokalnego zarządzania wdrożeniami na małą skalę przy pomocy urządzenia. Cisco Secure FMC, rozwiązanie lokalne przeznaczone do dużych wdrożeń, umożliwia centralne zarządzanie zdarzeniami i zasadami dotyczącymi zabezpieczeń, oferuje ponadto bogate opcje raportowania i lokalną rejestrację. CDO to chmurowy menedżer zabezpieczeń, który usprawnia zasady bezpieczeństwa i zarządzanie urządzeniami w całej rozbudowanej sieci. Natomiast Cisco Security Analytics and Logging zapewnia skalowalną kontrolę dzienników z analizą zachowań.

Historie klientów | Demo

Zaawansowane możliwości Cisco Secure Firewall:

Zaawansowane możliwości	Szczegóły
Integracja z Cisco Secure Workload	• Integracja z Cisco Secure Workload (Tetration) gwarantuje wszechstronny wgląd i egzekwowanie zasad w nowoczesnych rozwiązaniach rozproszonych i dynamicznych w całej sieci i przy dużym obciążeniu, zapewniając spójne przestrzeganie reguł w skalowalny sposób.
Zaawansowana analiza zagrożeń (Talos)	• Talos stanowi podstawę ekosystemu zabezpieczeń Cisco, chroniąc infrastrukturę organizacji przed złośliwym oprogramowaniem i nieznanymi zagrożeniami.
Cisco Defense Orchestrator CDO	• Ta oparta na chmurze aplikacja pomaga spójnie zarządzać zasadami we wszystkich produktach zabezpieczających Cisco.
Cisco Security Analytics and Logging	• Wysoce skalowalne zarządzanie dziennikami z analizą behawioralną, które służy do wykrywania zagrożeń w czasie rzeczywistym, by skrócić czasy reakcji i umożliwić ciągłą analitykę w celu dalszej poprawy bezpieczeństwa, a w rezultacie – zapewnienia lepszej ochrony przed przyszłymi zdarzeniami stwarzającymi zagrożenia.
	• Globalna, ciągła analiza zagrożeń i zabezpieczenia retrospektywne, a także wykrywanie i blokowanie złośliwego oprogramowania w określonym punkcie w czasie.
Next-Generation Intrusion Prevention System (SNORT)	• Wiodący w branży system nowej generacji o otwartym kodzie źródłowym (NGIPS) mający na celu zapobieganie nieautoryzowanemu dostępowi. Zapewnia zwiększoną ochronę przed nawet najbardziej wyrafinowanymi zagrożeniami, pomagając organizacjom w przestrzeganiu wymogów prawnych.
Reakcja na zagrożenie SecureX	• Korzystając z informacji o zagrożeniach uzyskanych w wyniku analizy Talos, rozwiązanie to automatycznie bada wskaźniki naruszeń bezpieczeństwa i szybko potwierdza zagrożenia.

Dalsze kroki

Więcej informacji o Secure Firewall znaleźć można na stronie cisco.com/go/ngfw.

Aby zapoznać się z opcjami zakupu i porozmawiać z przedstawicielem handlowym Cisco, zapraszamy na www.cisco.com/c/en/us/buy.