

## Urządzenia Cisco z serii ASA 5500 – Informacje

Adaptacyjne urządzenia zabezpieczające z serii Cisco® ASA 5500 to modularna platforma udostępniająca najnowszej generacji zabezpieczenia i usługi VPN dla środowisk o różnej wielkości – od domów i małych biur, przez małe i średnie przedsiębiorstwa, po duże korporacje. Urządzenia z serii Cisco ASA 5500 oferują przedsiębiorstwom szeroki zakres usług, dostosowywanych za pomocą różnych wersji produktów przeznaczonych do współdziałania z zaparami, blokowania dostępu intruzów, działań anti-X i sieci VPN.

Różnorodność wersji zapewnia doskonałą ochronę i właściwe pakiety usług dla wszystkich sytuacji. Każda wersja zawiera wyspecjalizowany zestaw usług Cisco ASA spełniający potrzeby konkretnych obszarów sieci korporacyjnych. Dzięki spełnieniu potrzeb związanych z bezpieczeństwem poszczególnych lokalizacji, zwiększone zostaje bezpieczeństwo całej sieci.



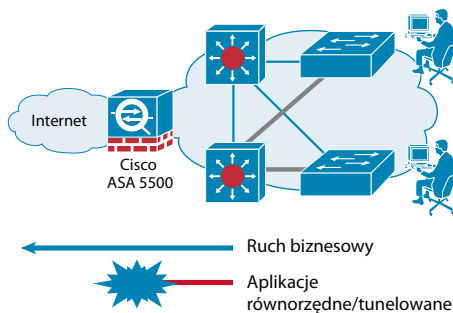
Urządzenia z serii Cisco ASA 5500 zapewniają standaryzację usług na jednej platformie, co pozwala na zmniejszenie łącznego kosztu operacyjnego zabezpieczeń. Wspólne środowisko konfiguracyjne upraszcza zarządzanie i zmniejsza koszty szkolenia pracowników, a wspólna platforma sprzętowa serii zmniejsza koszty części zamiennych.

Poszczególne wersje spełniają potrzeby różnych środowisk korporacyjnych:

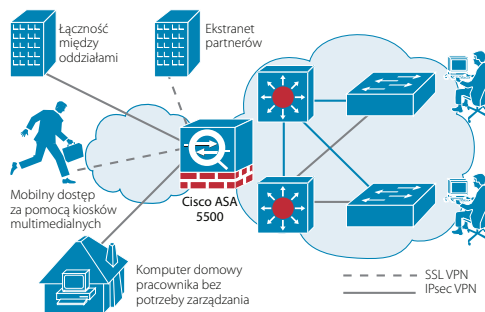
- Wersja Firewall Edition: Zapewnia firmom możliwość bezpiecznego i niezawodnego wdrażania najważniejszych aplikacji i sieci. Unikalna, modularna architektura zapewnia wysoki poziom ochrony inwestycji i zmniejszony koszt eksploatacji.
- Wersja IPS Edition: Chroni najważniejsze dla firmy serwery i infrastrukturę przed robakami internetowymi, hakerami i innymi zagrożeniami poprzez połączenie usług zapory, bezpieczeństwa aplikacji i blokowania dostępu intruzów.
- Wersja Anti-X Edition: Chroni użytkowników niewielkich i zdalnych lokalizacji za pomocą bogatego pakietu usług bezpieczeństwa. Zapora i usługi VPN klasy korporacyjnej zapewniają bezpieczną łączność z główną siedzibą korporacji. Wiodące usługi typu anti-X firmy Trend Micro chronią systemy klienckie przed złośliwymi witrynami WWW i niebezpieczną zawartością, taką jak wirusy, programy szpiegujące i witryny wyludzające informacje.

- Wersja SSL/IPsec VPN Edition: Zapewnia użytkownikom bezpieczny, zdalny dostęp do systemów i usług sieci wewnętrznej oraz obsługuje łączenie sieci VPN w klastry przy wdrożeniach w dużych przedsiębiorstwach. Technologie dostępu zdalnego VPN Secure Sockets Layer (SSL) i IP Security (IPsec) połączone z technologiami zmniejszania zagrożenia, takimi jak Cisco Secure Desktop, oraz usługami zapory i blokowaniem dostępu intruzów dają pewność, że ruch w sieci VPN nie stanowi zagrożenia dla przedsiębiorstwa.

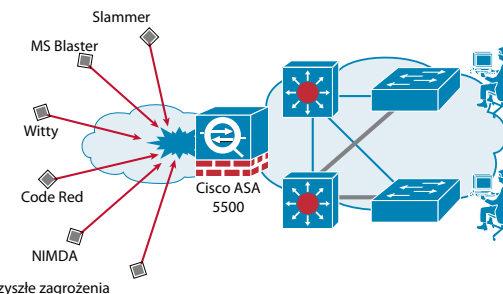
## Wiodące na rynku zabezpieczenia aplikacji



## Bezpieczne usługi VPN SSL i IPsec



## Wiodące na rynku usługi IPS/Anti-X



## 5 najważniejszych powodów rozważenia zakupu adaptacyjnych urządzeń zabezpieczających z serii Cisco ASA 5500

- Zaufana technologia zapory i chronionych sieci VPN.**  
Zbudowane na zaufanej technologii urządzeń zabezpieczających Cisco PIX® i koncentratorów z serii Cisco VPN 3000. Urządzenia z serii Cisco ASA 5500 to pierwsze na rynku rozwiązanie oferujące usługi SSL i IPsec VPN chronione przez doskonałą zapórę.
- Wiodące na rynku usługi Anti-X**  
Łącząc doświadczenie firmy Trend Micro w dziedzinie ochrony przez zagrożeniami i kontrolowania treści na styku z Internetem ze sprawdzonymi technologiami firmy Cisco, zapewniając rozbudowane usługi antywirusowe, ochronę przed programami szpiegującymi, blokowanie plików, ochronę przed spamem i witrynami wyludzającymi informacje, blokowanie i filtrowanie adresów URL oraz filtrowanie treści.
- Zaawansowane usługi blokowania dostępu intruzów**  
Zapewniają aktywne, bogate usługi blokowania dostępu intruzów powstrzymujące wiele zagrożeń, w tym robaki internetowe, ataki w warstwie aplikacji, ataki na poziomie systemu operacyjnego, programy rootkit, programy szpiegujące, współdzielenie plików P2P i komunikatory internetowe.
- Doskonałe usługi zarządzania i monitorowania**  
Zapewnia intuicyjne zarządzanie i monitorowanie poszczególnych urządzeń za pomocą narzędzia Cisco Adaptive Security Device Manager (ASDM) oraz korporacyjnej klasy usługi zarządzania wieloma urządzeniami za pomocą zestawu Cisco Security Management Suite.
- Zmniejszony koszt wdrożenia i eksploatacji**  
Poprzez udostępnienie architektury i interfejsu zgodnego z dostępnymi rozwiązaniami bezpieczeństwa firmy Cisco, urządzenia z serii Cisco ASA 5500 umożliwiają znaczne zmniejszenie kosztów początkowego wdrożenia systemu bezpieczeństwa i codziennego zarządzania.



# Adaptacyjne urządzenia zabezpieczające z serii Cisco ASA 5500

W skrócie

**SKRÓTY**  
**SSC:** Security Services Card (Karta usług bezpieczeństwa), **SSM:** Security Services Module (Moduł usług bezpieczeństwa), **AIP-SSM:** Advanced Inspection and Prevention Security Services Module (Zaawansowany moduł usług badania i zapobiegania),  
**CSC-SSM:** Content Security and Control Security Services Module (Moduł usług bezpieczeństwa i kontroli treści), **4GE-SSM:** 4 Gigabit Ethernet Security Services Module (Moduł usług bezpieczeństwa sieci Ethernet 4Gb)

Model/licencja z serii Cisco ASA 5500	Cisco ASA 5505 Base/Security Plus	Cisco ASA 5510 Base/Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Rynek	SOHO/ROBO/MSSP/Pracownicy zdalni	Małe i średnie przedsiębiorstwa, niewielkie korporacje	Niewielkie korporacje	Średniej wielkości korporacje	Duże korporacje
<b>Podsumowanie możliwości</b>					
Maksymalna przepustowość zapory (Mb/s)	150	300	450	650	1200
Maksymalna przepustowość 3DES/AES sieci VPN (Mb/s)	100	170	225	325	425
Maksymalna liczba sesji między biurami i zdalnego dostępu VPN	10/25	250	750	5000	5000
Maksymalna liczba sesji SSL sieci VPN <sup>1</sup>	25	250	750	2500	5000
Maksymalna liczba połączeń	10 000/25 000	50 000/130 000	280 000	400 000	650 000
Maksymalna liczba połączeń na sekundę	3000	6000	9000	20 000	28 000
Pakiety na sekundę (64 bajty)	85 000	190 000	320 000	500 000	600 000
<b>Podsumowanie techniczne</b>					
Pamięć (MB)	256	256	512	1024	4096
Pamięć flash systemu (MB)	64	64	64	64	64
Wbudowane porty	8-portowy przełącznik 10/100 z 2 portami Power over Ethernet	5-10/100	4-10/100/1000, 1-10/100	4-10/100/1000, 1-10/100	8-10/100/1000, 1-10/100
Maksymalna liczba interfejsów wirtualnych (VLAN)	3 (trunking wyłączony) / 20 (trunking włączony)	50/100	150	200	250
Gniazdo rozszerzeń SSC/SSM	Tak (SSC)	Tak (SSM)	Tak (SSM)	Tak (SSM)	Nie
<b>Możliwości SSC/SSM</b>					
Obsługiwane urządzenia SSC/SSM	Future, SSC	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	Nie
Blokowanie dostępu intruzów	Niedostępne	Tak (z AIP-SSM)	Tak (z AIP-SSM)	Tak (z AIP-SSM)	Nie
Współbieżna przepustowość zmniejszania zagrożenia (Mb/s) (zapora + usługi IPS)	Niedostępne	150 (z AIP-SSM-10) 300 (z AIP-SSM-20)	225 (z AIP-SSM-10) 375 (z AIP-SSM-20)	450 (z AIP-SSM-20)	Niedostępne
Usługi anti-X (ochrona przed wirusami, programami szpiegującymi, spamem i wityrnymi wyłudżającymi informacje, blokowanie plików, filtrowanie adresów URL)	Niedostępne	Tak (z CSC-SSM)	Tak (z CSC-SSM)	Tak (z CSC-SSM)	Niedostępne
Maksymalna liczba użytkowników usług ochrony przed wirusami i programami szpiegującymi oraz blokowania plików (tylko CSC-SSM)	Niedostępne	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	Niedostępne
Funkcje licencji CSC SSM Plus	Niedostępne	Ochrona przed spamem i wityrnymi wyłudżającymi informacje, filtrowanie adresów URL	Ochrona przed spamem i wityrnymi wyłudżającymi informacje, filtrowanie adresów URL	Ochrona przed spamem i wityrnymi wyłudżającymi informacje, filtrowanie adresów URL	Niedostępne
<b>Funkcje</b>					
Bezpieczeństwo warstwy aplikacji	Tak	Tak	Tak	Tak	Tak
Transparentna zapora w warstwie 2	Tak	Tak	Tak	Tak	Tak
Konteksty zabezpieczeń (dołączone/maksymalnie) <sup>2</sup>	0/0	0/0 / 2/5	2/20	2/50	2/50
Badanie GTP/GPRS <sup>2</sup>	Niedostępne	Niedostępne	Tak	Tak	Tak
Obsługa wysokiej dostępności <sup>3</sup>	Brak obsługi/Bezstanowe A/S	Niedostępna / A/A i A/S	A/A i A/S	A/A i A/S	A/A i A/S
Łączenie sieci VPN w klastry i równoważenie obciążenia	Niedostępne	Niedostępne	Tak	Tak	Tak

<sup>1</sup> Poczwszy od wersji 7.1 oprogramowania Cisco ASA Software obsługa SSL VPN (WebVPN) wymaga licencji. Systemy domyślnie mają obsługę 2 użytkowników SSL VPN do celów ewaluacji i zarządzania zdalnego.

<sup>2</sup> Funkcje licencjonowane

<sup>3</sup> A/S = Active/Standby (Aktywny/Oczekiwanie); A/A = Active/Active (Aktywny/Aktywny)