Rozwiązanie SonicWall SMA

Możliwości

SonicWall SMA to zunifikowana brama, która zapewnia organizacjom bezpieczny dostęp do krytycznych zasobów korporacyjnych - w każdym momencie, z dowolnego urządzenia i miejsca.

- Dla organizacji chcących korzystać z zalet BYOD, elastycznego stylu pracy i bezpiecznej współpracy z niezależnymi podmiotami SMA staje się kluczowym narzędziem do egzekwowania bezpiecznego dostępu.
- Dla organizacjji rozpoczynających swoją migrację do chmury SMA oferuje infrastrukturę jednokrotnego logowania (SSO), która korzysta z pojedynczego portalu webowego do uwierzytelniania użytkowników w hybrydowym środowisku IT.
- Dla organizacji hostujących własną infrastrukturę, a także dostawców usług zarządzanych SMA to kompleksowe rozwiązanie zapewniające wysoki poziom ciągłości biznesowej oraz dużą skalowalność.

Problemy i potrzeby klienta

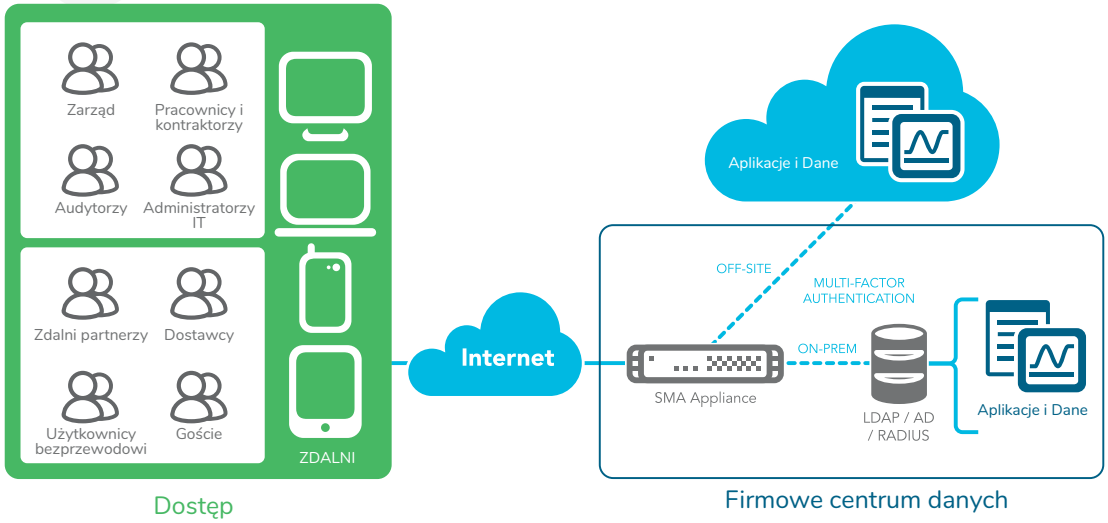
- Chcę zapewnić pracownikom mobilnym niezawodny i bezpieczny dostęp do krytycznych aplikacji z dowolnego autoryzowanego urządzenia
- Chcę kontrolować wszystkie urządzenia mobilne łączące się z moją siecią, zarówno te używane w ramach modelu BYOD, jak i zarządzane przez dział IT
- Muszę ograniczyć dostęp VPN do aplikacji mobilnych związanych z biznesem
- Muszę uprościć infrastrukturę dostępową w moim hybrydowym środowisku IT podczas migracji aplikacji do chmury
- Chcę zapewnić bezpieczne jednokrotne logowanie (SSO) do dowolnej aplikacji w sieci lub w chmurze przy użyciu jednego adresu URL
- Muszę zapewnić moim zdalnym pracownikom bezpieczny sposób przesyłania i udostępniania plików
- Muszę zapobiegać nieautoryzowanemu dostępowi do firmowych aplikacji, danych i zasobów z zagubionych lub skradzionych urządzeń mobilnych
- Chcę zapewniać dostępność usług 24x7 i spełniać rygorystyczne warunki umów SLA

Właściwi odbiorcy

1. Administratorzy IT, CIO, CISO, CSO, specjaliści ds. bezpieczeństwa, specjaliści ds. zgodności z przepisami, osoby zarządzające finansami firmy, właściciele firm.
2. Segmenty
   - Klienci ze średnich i dużych przedsiębiorstw i instytucji
   - Dostawcy usług zarządzanych (MSP) i chmurowych
   - Obecni klienci SonicWall

Zalety SonicWall – dlaczego rozwiązanie SMA?

- SonicWall automatycznie i w czasie rzeczywistym wykrywa i zapobiega naruszeniom bezpieczeństwa, wykorzystując wielosilnikowy, oparty na chmurze sandboxing, który jest dostępny w całym portfolio produktów
- Nadzór na tym, kto ma dostęp do jakich zasobów, z możliwością definiowania szczegółowych polityk w oparciu o zaawansowany, obiektowy mechanizm kontroli dostępu
- Wgląd w każde łączące się urządzenie i możliwość udzielania dostępu na podstawie polityk i stanu ochrony punktu końcowego
- Bezpieczny dostęp, oparty na natywnej funkcjonalności agenta w przeglądarce HTML5, który nie wymaga instalowania i utrzymywania agentów na urządzeniach końcowych
- Większa wydajność pracowników dzięki jednokrotnemu logowaniu (SSO) do dowolnej usługi SaaS lub aplikacji hostowanej lokalnie przy użyciu jednego adresu URL
- Blokowanie ataków DDoS i zombie za pomocą filtrów Geo IP i anty-Botnet
- Ochrona przed atakami webowymi i zapewnianie zgodności ze standardem PCI dzięki dodatkowemu rozwiązaniu Web Application Firewall
- Możliwość dynamicznego wydawania licencji dostępu zgodnie ze zmieniającymi się w czasie rzeczywistym potrzebami oraz wbudowany mechanizm równoważenia obciążeń
- Niższy całkowity koszt posiadania i ograniczenie złożoności zarządzania dostępem poprzez konsolidację komponentów infrastruktury w hybrydowym środowisku IT



Rozwiązanie SMA zapewnia bezpieczny dostęp wszystkim użytkownikom, urządzeniom i aplikacjom.

*Dostępne w wybranych modelach SMA, wyszczególnionych w tabeli porównawczej.

Rozwiązanie SonicWall SMA

Pytania kwalifikacyjne

- Czy migrujesz do chmury? Czy używasz Salesforce, Office 365 lub Concur?
- Czy Twoi pracownicy, dostawcy lub kontrahenci działają zdalnie?
- Czy Twoi pracownicy zarządzają wieloma adresami URL i hasłami?
- Czy chcesz wdrożyć bezpieczne logowanie jednokrotne (SSO) i uwierzytelnianie wieloskładnikowe?
- Czy posiadasz strategię bezpiecznego dostępu do hybrydowego środowiska IT?
- Czy Twoi pracownicy używają usługi Dropbox lub osobistego adresu e-mail do udostępniania plików firmowych?
- Jaka jest Twoja obecna strategia mobilności/BYOD?
- Czy masz wgląd w każde urządzenie, które uzyskuje dostęp do Twojej sieci?
- W jaki sposób kontrolujesz i zabezpieczasz dostęp do określonych aplikacji z urządzeń mobilnych?
- Czy skanujesz wszystkie pliki przychodzące do sieci za pośrednictwem SSL VPN?
- Czy musisz zapewnić dostęp 24x7 i ciągłość usług?
- Czy korzystasz z więcej niż jednego centrum danych?

Konkurencja/różnice

Pulse Secure (poprzednio Juniper SA/MAG)

- Pulse Secure wymaga modyfikacji aplikacji mobilnych przy użyciu specjalnego pakietu SDK w celu wykorzystania kontroli dostępu VPN na poziomie aplikacji
- Brak metody egzekwowania polityk autoryzacji i rejestracji urządzeń osobistych
- Brak integracji z rozwiązaniem Sandbox

Odpowiedź

- Od wersji 11.x system SonicWall SMA OS zapewnia kontrolę mobilnego dostępu VPN na poziomie aplikacji, która nie wymaga modyfikacji przy użyciu SDK
- Umożliwia działowi IT zarządzanie i egzekwowanie polityk autoryzacji oraz rejestracji urządzeń osobistych
- System SMA 12.1 lub nowszy umożliwia integrację ochrony Capture ATP w celu bezpiecznego udostępniania plików
- Mniejszy całkowity koszt posiadania dzięki wbudowanemu mechanizmowi równoważenia obciążeń oraz elastycznym modelom licencjonowania

---

Cisco ASA z AnyConnect

- SSL VPN jest dodatkową nie podstawową funkcją
- Licencjonowanie i zarządzanie SSL VPN jest kosztowne i złożone
- Brak integracji z rozwiązaniem Sandbox

Odpowiedź

- Specjalnie zaprojektowana brama, która zapewnia w każdym momencie bezpieczny dostęp z dowolnego urządzenia do dowolnej aplikacji
- Dzięki ujednoliconej kontroli nad politykami rozwiązania SonicWall SMA są bardzo ekonomiczne
- i łatwe w zarządzaniu
- Dział IT może zarządzać i egzekwować polityki autoryzacji i rejestracji urządzeń osobistych oraz dostęp VPN na poziomie aplikacji
- System SMA 12.1 lub nowszy umożliwia integrację ochrony Capture ATP w celu bezpiecznego udostępniania plików

---

Korzyści z wdrożenia SMA

- Większa wydajność
- Zwiększona przepustowość
- Zaawansowane funkcje
- Lepsza skalowalność

Zestawienie funkcjonalności (według modelu SMA)

Kategoria	Funkcja	210	410	500v	6210	7210	8200v
Przepustowość	Maks. liczba jednoczesnych sesji użytkowników	50	250	250	2,000	10,000	5,000
	Maks. przepustowość SSL/TLS	560 Mb/s	844 Mb/s	186 Mb/s	800 Mb/s	5.0 Gb/s	1.58 Gb/s
Dostęp kliencki	Layer 3 tunnel	•	•	•	•	•	•
	Split-tunnel and redirect-all	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•
	Auto ESP encapsulation	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Secure Network Detection	–	–	–	•	•	•
	File browser (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	On Demand tunnel	–	–	–	•	•	•
	Chrome/Firefox extensions	–	–	–	•	•	•
	CLI tunnel support	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows,Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Dostęp mobilny	Per app VPN	–	–	–	•	•	•
	App control enforcement	–	–	–	•	•	•
	App ID validation	–	–	–	•	•	•
Portal użytkownika	Branding	•	•	•	•	•	•
	Customization	–	–	–	•	•	•
	Localization	•	•	•	•	•	•
	User defined bookmarks	•	•	•	•	•	•
	Custom URL support	•	•	•	•	•	•
	SaaS application support	–	–	–	•	•	•
Bezpieczeństwo	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	–	–	–	•	•	•
	Suite B ciphers	–	–	–	•	•	•
	Dynamic EPC interrogation	•	•	•	•	•	•
	Role Based Access Control (RBAC)	–	–	–	•	•	•
	Endpoint registration	•	•	•	•	•	•
	Secure File Share (Capture ATP)	•	•	•	•	•	•
	Endpoint quarantine	•	•	•	•	•	•
	OSCP CRL validation	–	–	–	•	•	•
	Cipher selection	–	–	–	•	•	•
	PKI and client certificates	•	•	•	•	•	•
	Geo IP filter	•	•	•	–	–	–
	Botnet filter	•	•	•	–	–	–
	Forward proxy	•	•	•	•	•	•
	Reverse proxy	•	•	•	•	•	•
wierzytelnianie i usług oparte na tożsamości	SAML 2.0	–	–	–	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	–	–	–	•	•	•
	Biometric device support	•	•	•	•	•	•
	Face ID support for iOS	•	•	•	•	•	•
	Two-factor authentication (2FA)	•	•	•	•	•	•
	Multi-factor authentication (MFA)	–	–	–	•	•	•

Zestawienie funkcjonalności (według modelu SMA) cd.

Kategoria	Funkcja	210	410	500v	6210	7210	8200v
Uwierzytelnianie i usługi oparte na tożsamości cd.	Chained authentication	–	–	–	●	●	●
	One Time Passcode(OTP) via email or SMS	●	●	●	●	●	●
	Common Access Card (CAC) support	–	–	–	●	●	●
	X.509 certificate support	●	●	●	●	●	●
	Captcha integration	–	–	–	●	●	●
	Remote password change	●	●	●	●	●	●
	Forms based SSO	●	●	●	●	●	●
	Federated SSO	–	–	–	●	●	●
	Session persistence	–	–	–	●	●	●
	Auto logon	●	●	●	●	●	●
Kontrola dostępu	Group AD	●	●	●	●	●	●
	LDAP attributes	●	●	●	●	●	●
	Geolocation policies	●	●	●	–	–	–
	Continual endpoint monitoring	●	●	●	●	●	●
Zarządzanie	Management interface (ethernet)	–	–	–	●	●	●
	Management interface (console)	–	–	–	●	●	●
	HTTPS administration	●	●	●	●	●	●
	SSH administration	–	–	–	●	●	●
	SNMP MIBS	●	●	●	●	●	●
	Syslog and NTP	●	●	●	●	●	●
	Usage monitoring	●	●	●	●	●	●
	Configuration rollback	●	●	●	●	●	●
	Centralized management	–	–	–	●	●	●
	Centralized reporting	–	–	–	●	●	●
	Management REST APIs	–	–	–	●	●	●
	Authentication REST APIs	–	–	–	●	●	●
	RADIUS accounting	–	–	–	●	●	●
	Scheduled tasks	–	–	–	●	●	●
	Centralized session licensing	–	–	–	●	●	●
	Event-driven auditing	–	–	–	●	●	●
Sieć	IPv6	●	●	●	●	●	●
	Global load balancing	–	–	–	●	●	●
	Server load balancing	●	●	●	–	–	–
	TCP state replication	●	●	●	●	●	●
	Cluster state failover	–	–	–	●	●	●
	Active/passive high availability	–	●	●	●	●	●
	Active/active high availability	–	–	–	●	●	●
	Horizontal scalability	–	–	–	●	●	●
	Single or multiple FQDNs	–	–	–	●	●	●
	L3-7 smart tunnel proxy	●	●	●	●	●	●
	L7 application proxy	●	●	●	●	●	●
Integracja	2FA TOTP support	●	●	●	●	●	●
	EMM and MDM product support	–	–	–	●	●	●
	SIEM product support	–	–	–	●	●	●
	TPAM password vault	–	–	–	●	●	●
	ESX hypervisor support	–	–	●	–	–	●
	Hyper-V hypervisor support	–	–	●	–	–	●
Opcje licencyjne	Subscription based license	–	–	–	●	●	●
	Perpetual license with support	●	●	●	●	●	●
	Web Application Firewall (WAF)	●	●	●	–	–	–
	Spike licensing	●	●	●	●	●	●
	Tiered licensing	–	–	–	●	●	●
	Virtual assist	●	●	●	–	–	–

** Więcej informacji o klientach VPN na stronie: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*