Firewall nowej generacji SANGFOR (NGFW)

Ochrona nowej generacji dla twojego biznesu

Firewall nowej generacji SANGFOR został tak zaprojektowany, z myślą o kontroli aplikacji, zapobieganiu włamaniom i ochronie stron internetowych, w celu zapewnienia doskonałej widoczności użytkowników, aplikacji i treści. SNAGFOR NGFW zapewnia pełną ochronę w warstwach od 2 do 7 z prędkością wielu gigabitów czym odróżnia się od tradycyjnych firewalli i co czyni go idealnym wyborem dla klientów.

Ochrona całych aplikacji
Dwukierunkowa kontrola zawartości
Inteligentny system ochrony
Wysoka wydajność warstwy aplikacji

Cechy produktu

Kompleksowa ochrona	
Firewall	Statyczne i dynamiczne filtrowanie pakietów. Kontrola znanych protokołów FTP, HTTP, SMTP, RTSP, H.323 (Q.931, H.245, RTP/RTCP), SQLNET, NMS, PPTP, TCP, UDP… Ochrona przed atakami Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP spoofing, SYN/ICMP/powódź UDP, powódź HTTP GET, powódź zapytań DNS, oszustwo ARP, przekierowywanie ICMP, statyczna i dynamiczna czarna lista, itp.
Ochrona przed wtargnięciem	Skanowanie na podstawie sygnatur, protokołów lub aplikacji. Inteligentna analiza nieznanych zagrożeń dzieki analizie korelacyjnej. Aktualny certyfikat zgodności CVE z bazą danych IPS zawierającą ponad 3000 sygnatur. Baza danych sygnatur serwerów i grup terminali dla elastycznej polityki wdrażania. Poltyka ochrony IPS oparta na źródłowym / docelowym IP i podsieci. Blokuje robaki, trojany, spyware, skanowanie DoS, DdoS, wykorzystywanie luk, ataki przepełniania buforu, nienormalne protokoły i ataki wykorzystujące taktykę ucieczki. Szczegółowe powiadomienia o logach i analiza zagrożeń w chmurze.
Anty wirus	Anty wirus oparty na strumieniu dla HTTP, FTP, SMTP i POP3, protokołów, itp. Aktualizowana na bieżąco ręcznie lub automatycznie baza danych zawierająca ponad 300 000 sygnatur wirusów. Wbudowana baza anty wirusa i silnik SOPHOS.
Ochrona aplikacji sieciowych	Aktualna baza danych pona 2000 sygnatur zagrożeń sieciowych. Czarna lista i lista wykluczeń URL. Ochrona słabych haseł dla ftp i telnetu, itp. Ochrona aplikacji internetowych przed dziesięcioma najpoważniejszymi zagrożeniami zdefiniowanymi przez OWASP, w tym iniekcja SQL, atak XSS, CRSF, itp. Informacje o serwerze są niewidzialne dla serwera sieciowego, serwera ftp, itp. Skanowanie i filtrowanie wgrywanych plików w oparciu o sygnatury.
DLP	Wbudowana baza sygnatur wrażliwych informacji i wsparcie ochrony zdefiniowanych przez użytkownika informacji poufnych, takich jak; nazwa użytkownika, hasło, skrzynka pocztowa, ID i klucze MD5. Zapobiega wyciekowi informacji przez połaczenia HTTP. Zapewnia wysoki poziom bezpieczeństwa wrażliwych informacji w bazie danych, chroni przed wyciekiem danych.
Ocena ryzyka	Skanowanie portów i usług dla niektórych IP, ocena ryzyka dla serwrów i terminali. Wspomaga słabe hasła dla FTP, MYSQL, ORACLE, MSSQL, SSH, RDP, NetBIOS i usług VNC, itp. Automatycznie generuje między modułową politykę bezpieczeństwa dla modułó FW, PS i WAF, aby zapewnić pełną ochronę.

Uwierzytelnianie i widoczność	
Uwierzytelnianie użytkownika	Mapowanie poprzez IP, MAC, wiązane IP/MAC, nazwę hosta i klucz USB. Importowanie kont użytkowników z pliku CSV i serwera LDAP. Bezproblemowa integracja z AD i LDAP, polityka oparta na integracji z SSO, domeną AD, proxy, POP3 i WEB.
Kontrola aplikacji	Identyfikacja aplikacji oparta na bazie dznych sygnatur aplikacji. Obsługa polityki kontroli opartej na aplikacjach.
Filtrowanie URL	Dyskowa baza danych URL, technologia anty proxy. Obsługuje politykę opartą na kategoriach i grupach.
Widoczność HW&SW	Monitoring w czasie rzeczywistym pracy procesora, pamięci, dysku, sesji, użytkowników i informacje dotyczące interfejsu sieci.
Widoczność BM	Rankigowanie według IP wykorzystania przepustowości, aplikacji i użytkowników.
Widoczność bezpieczeństwa	Szczegółowe informacje, w czasie rzeczywistym na temat kwestii bezpieczeństwa serwerów lub terminali, włącznie z źródłowym/docelowym adresem IP, kategorią ataku i URL, itp.

Sieciowanie i optymalizacja	
Wdrożenie	Bramka, most, tryb obejścia, wirtualne połączenie i tryb mieszany.
Sieć	Obsługa ARP, DNS, IP UNNUMBERED. Polityka wspierania routingu, routing statyczny, RIP vl/2 i OSPF Obsługa przekazywania opartego na aplikacjach.
NAT	1:1 NAT, n:n NAT, m:n NAT, poltyka NAT oparta na czasie. Obsługa NAT ALG, wraz z DNS, FTP, H.323 i SIP, itp.
Wbudowany IPsec VPN	Wbudowany IPsec VPN oparty na trasie, dla bezpiecznego, szybkiego i taniego wdrażania zdalnej sieci biurowej.
Zarządzanie przepustowością	Wsparcie multipleksowania i inteligentny routing. Zaawansowana kontrola P2P. Polityka QoS oparta na użytkownikach, aplikacjach, IP, typach plików, typach stron, harmonogramch, itp.

Zarządzanie	
Zarządzanie	Obsługa sieciowego GUI z kodowaniem SSL; Obsługa SNMP.
Alarmy	Obsługa E-mail, alarmy MSM na znak, wirusów, IPS, ataków sieciowych i problemów sprzętowych. Obsługa narzedzi graficznych do rozwiązywania problemów.
Konfiguracja	Obsługa szablonów konfiguracji dla ułatwienia konserwacji.

Raportowanie	
Raport zagrożeń	Raport zagrożeń bezpieczeństwa w oparciu o porty, usługi, słabości i słabe hasła zapewnia wytyczne dla administratora IT.
Dziennik zabezpieczeń	Szczegółowe dzienniki zdarzeń, takich jak atak DOS, atak sieciowy, IPS, wirusy, dostęp do strony, kontrola aplikacji, login użytkownika i konfiguracja OS.
Raport trendów	Obsługuje raport trendów w oparciu o harmonogram.
Raport statystyk	Tworzy raporty w elastycznym harmonogramie, według określonych przez użytkownika statystyk, w oparciu o IP, grupy, użytkowników, aplikacje.
Format raportów	Obsługuje format XML, PDF i automatycznie wysyła do użytkowników z określonej listy emailowej.

SANGFOR

Firewall nowej generacji SANGFOR (NGFW)

Rodzina produktów

Model	S5000-F-I	M5000-F-I	M5100-F-I	M5200-F-I	M5300-F-I	M5400-F-I	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I
Profil	Mini	1U	1U	1U	1U	1U	2U	2U	2U	2U
RAM	2G	2G	2G	2G	2G	4G	4G	8G	16G	24G
Pojemność dysku	320GB	320GB	320GB	320GB	320GB	320GB	500GB	500GB	500GB	500GB
Przepustowość Firewalla	1 Gb/s	1 .5 Gb/s	2 Gb/s	3 Gb/s	5 Gb/s	8 Gb/s	12 Gb/s	18 Gb/s	20 Gb/s	25 Gb/s
Przepustowość Firewalla (włączone APP &URL)	50 Mb/s	100 Mb/s	200 Mb/s	400 Mb/s	500 Mb/s	700 Mb/s	1Gb/s	2 Gb/s	5 Gb/s	10 Gb/s
Przepustowość PS	35 Mb/s	70 Mb/s	100 Mb/s	150 Mb/s	300 Mb/s	500 Mb/s	650 Mb/s	1.3 Gb/s	3.8 Gb/s	6.8 Gb/s
Przepustowość WAF	20 Mb/s	50 Mb/s	70 Mb/s	100 Mb/s	200 Mb/s	400 Mb/s	550 Mb/s	1 Gb/s	2.5 Gb/s	5 Gb/s
Nowe sesje na sekundę	10,000	11,000	13,000	20,000	30,000	50,000	90,000	150,000	200,000	300,000
Maksymalna liczba jednoczesnych sesji	500,000	1,000,000	1,200,000	1,500,000	1,800,000	2,100,000	2,300,000	6,000,000	8,000,000	15,000,000

Zasilanie i specyfikacja fizyczna

Podwójne zasilacze	Nie	Nie	Nie	Nie	Nie	Nie	Tak	Tak	Tak	Tak
Moc [Watt] (Typowa)	60 W	60 W	60 W	100 W	100 W	250 W	300 W	300 W	500 W	500 W
Temperatura	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C
Wilgotność względna	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji	5%~95% bez kondensacji
Wymiary systemu (Szer. x Dłu. x Wys. mm)	275 x 175 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 430 x 44.5	440 x 500 x 89	440 x 500 x 89	440 x 500 x 89	440 x 600 x 90
Waga systemu	1.5 Kg	3.9 Kg	4.0 Kg	4.2 Kg	4.25 Kg	7.0 Kg	10.9 Kg	18.0 Kg	19.0 Kg	20.0 Kg

Interfejsy sieciowe

Obejście (miedź)	Nie	Nie	1 para	1 para	1 para	1 para	2 pary	3 pary	4 pary	4 pary
10/100/1000	3	4	4	6	4	8	8	10	8	8
1G światłowód SFP	-	-	-	-	2	-	2	4	4	-
10G światłowód SFP	-	-	-	-	-	-	-	-	-	2

IT FORCE

Wyłączny Dystrybutor Sangfor Technologies w Polsce:
IT FORCE SP. z o.o.
ul. Fredry 2, 30-605 Kraków,
tel. 12 36 12121 **www.itforce.com.pl**