

Porównanie UTM 2021

ikaria	Opis	Barracuda NG	Checkpoint	Cisco ASA FIREPOWER	Dell Sonicwall	Fortinet	Intel Security (McAfee) FORCEPOINT	Juniper	PaloAlto	Stormshield	Sophos	WatchGuard Firebox
Podstawowe funkcje ochronne												
Firewall	Rodzaj firewalla	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter	statefull packet filter
AV	Czy jest zintegrowany moduł Antywirusowy	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
AV dostawca	Producent baz antywirusowych	Avira / ClamAV	Kaspersky + własny	CISCO AMP	McAfee	własny	McAfee	Sophos lub Kaspersky	własny - silnik Wildfire	Kaspersky/ClamAV	Sophos/ClamAV	AVG
IPS	Wbudowany system ochrony przed włamaniami, exploitami	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Antyspam	Wbudowany moduł filtrowania poczty (spamu)	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Filtrowanie URL	Możliwość filtrowania złośliwych stron	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
URL dostawca baz	Producent baz złośliwych URL	Proventia Internet Database	własne	SourceFire	własny	własny	webroot	Websense	własny	własne	własny	websense
Zaawansowane funkcje ochronne												
Https scanning	Możliwość skanowania szyfrowanego ruchu http	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Application Control	Kontrola aplikacji/firewall aplikacyjny	tak	tak	tak z asa cx	tak	tak	nie	w nowych modelach - AppTrack	tak - AppID	tak	tak	tak
DLP	Zabezpieczenie przed wyciekami danych	nie	tak	tak	nie	tak	nie	nie	tak	nie	tak	tak
Sandboxing	Piaskownica dla wykrywania nieznanymi/nierozpoznanych zagrożeń	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Generic DDoS	Ochrona przez atakami typu DDoS	tak	nie	tak	tak	tak	tak	tak	tak	tak	tak	tak
Reverse Proxy	Czy może funkcjonować jako reverse proxy	tak	tak	tak	nie	tak	tak - sso+vpn	tak	tak	nie ma	tak	tak/zachowuje się jak rp
VPN												
VPN Client	Dedykowane oprogramowanie dla VPN Client-To-Site	tak (NAC)	tak	tak	tak	tak (forticlient)	tak	tak (NetScreen) - płatny	tak - Global Protect	tak	tak - desktopy/mobilne	tak
VPN Site2Site	Możliwość tworzenia tuneli Site-To-Site	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Sieci bezprzewodowe												
Zintegrowany AP	Wbudowany moduł WiFi	tak	nie	tak w meraki	tak	tak	tak	nie	tak	nie	tak	nie
WiFi Controler	Możliwość zarządzania centralnego Access Pointami	nie	nie	tak w meraki	tak	tak	nie	nie	tak	nie	tak	nie/tak inna seria
3G/LTE	Wbudowane gniazdo na kartę SIM/port USB dla modemu	tak	tak - modemy producenta	nie	tak	tak	tak	tak - dużo różnych modeli niezależnych producentów	tak	tak, dedykowany modem	tak - kilka modeli	nie
Administracja												
Raportowanie	Możliwość tworzenia zestawień logów w formie tekstowej/graficznej	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Logowanie	Możliwość zbierania/przesyłania logów systemowych	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Interfejs zarządzania	Możliwość zarządzanie poprzez oprogramowanie, stronę WWW, konsolę	www/soft/CLI	www/CLI	soft/www/CLI	www/CLI	www/CLI	soft/www	www/CLI	www/CLI	www	www/CLI	www/CLI/soft
Autoryzacja użytkowników	Metody uwierzytelnienia dostępu do sieci firmowej:	lokalna,AD,LDAP,RADIUS,TACACS+, dwuetapowa przy ssl vpn	lokalna, AD, LDAP, RADIUS, dwuetapowa dla klientów mobilnych	lokalna,AD,LDAP,RADIUS,TACACS+,dwuetapowa	lokalna,AD,LDAP,RADIUS,dwuetapowa	lokalna,AD,LDAP,RADIUS,dwuetapowa - FortiToken	lokalna,AD,LDAP,RADIUS,dwuetapowa	lokalna,AD,LDAP,RADIUS,TACA CS+,dwuetapowa dla ssl vpn	lokalna,AD,LDAP,RADIUS,dwuetapowa	lokalna,AD,LDAP,RADIUS	lokalna,AD,LDAP,RADIUS	AD,LDAP,RADIUS, dwuetapowa dla ssl vpn
System operacyjny	Zainstalowany system operacyjny	Hardened Linux	własny	CISCO IOS	SonicOS	własny	własny	JunOS	PAN-OS	NETASQ Secured BSD	Hardened BSD	FIREWARE OS
Dostęp do systemu operacyjnego	Bezpośredni dostęp do plików urządzenia	tak	nie	nie	nie	nie	nie	tak	tak	tak	tak	nie
No CLI required	Nie trzeba używać wiersza poleceń do konfiguracji urządzenia	tak - ngadmin	tak	tak - asdm	tak	tak	tak	tak	tak	tak	tak	tak
Dostępność i niezawodność												
HA	Redundancja urządzeń/ Współdziałanie 2 lub więcej - rozłożenie mocy.	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Rendundacja zasilania	Nadmiarowość zasilaczy	tak	tak	tak	tak	tak	tak / FortiRPS	tak	tak	tak	tak	tak
Support	Rodzaj wsparcia technicznego	polski support	tak, angielski	j.ang, 90dni, mail, tel	polski	tak, mailowy, j.angielski	mail/tel, j.angielski	polski support	polski support	polski support	j.angielski	24x7
Virt. Appliance	Hypervisor dla maszyny wirtualnej jeżeli jest.	Vmware, NSX, Citrix, KVM, Amazon AWS, Microsoft Azure	Vmware, Hyper-V, Citrix, specjalna wersja dla NSXa, Amazon AWS, Azure	Vmware, NSX, Citrix, KVM, Amazon AWS, Microsoft Azure	nie	tak/esx, esxi, xen, centos,hyper-v,xen, aws,azure	Vmware, Oracle, KVM	vSRX - KVM, Vmware	Vmware, NSX, Citrix, KVM, Amazon AWS, Microsoft Azure	Vmware, citrix	Vmware, Amazon AWS, Azure	tylko Xtmv Vmware i hyper-v
Routing, kształtowanie ruchu												
App based routing	Zarządzanie ruchem w sieci wg aplikacji.	tak	nie	tak	nie	tak	nie	tak	tak	tak	tak	tak
App based QoS	Zarządzanie pasmem wg aplikacji.	tak	nie	tak	tak	tak	nie	tak	tak	nie	tak	nie
QoS	Kolejkowanie ruchu/ priorytetyzacja ruchu/ zarządzanie pasmem	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
WAN failover	Możliwość automatycznego przełączenia na zapasowego dostawcę internetu	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
WAN load balance	Równoważenie pasma internetu.	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak	tak
Poziom trudności instalacji	Zakładamy standardową instalację oraz że admin nie zna żadnego z rozwiązań.	trudny	łatwy	trudny	łatwy	łatwy	średni	trudny	średni	średni	średni	łatwy

Ikaria Ekspert Bezpieczeństwa IT

18 lat doświadczenia
1,5 milion chronionych komputerów
135 000 sprzedanych licencji
50 000 tysięcy klientów

Więcej informacji na www.ikaria.pl
Zadzwoń 42 680 82 33