

UTM-1

*Bezpieczeństwo, którego potrzebujesz;
prostota, jakiej oczekujesz*

WASZE WYZWANIA

Z powodu ciągle zmieniających się zagrożeń oraz nowych wyzwań, którym muszą sprostać zabezpieczenia, utrzymanie bezpieczeństwa sieci staje się coraz trudniejsze. Nowe produkty zabezpieczeń i zaimplementowane polityki, mające na celu sprostanie tej sytuacji znacząco podniosły złożoność, a co ważniejsze, koszty zabezpieczenia sieci i użytkowników. Potrzebne jest jednolite rozwiązanie, które gwarantuje wysoki poziom bezpieczeństwa, a jednocześnie zmniejsza ogólną złożoność i koszty.

NASZE ROZWIĄZANIE

Urządzenia UTM-1™ oferują sprawdzone, ściśle zintegrowane zabezpieczenia, które tworzą doskonałą mieszankę prostoty i bezpieczeństwa. Bazujące na tych samych technologiach CheckPoint, które zabezpieczają firmy z listy Fortune 500, urządzenia UTM-1 zapewniają bezkonkurencyjne bezpieczeństwo, a jednocześnie upraszczają instalację i administrację.

Urządzenia UTM-1 oferują kompletny zestaw funkcji zabezpieczeń zawierający zaporę firewall, system przeciwdziałania włamaniom (*Intrusion Prevention System* IPS), antywirusowy, anty-spyware, zaporę firewall dla aplikacji internetowych, zabezpieczenia ruchu VoIP, komunikatorów, a także blokowanie aplikacji P2P, filtrowanie treści WWW oraz bezpieczna łączność pomiędzy odległymi lokalizacjami i zdalny dostęp.

Urządzenia UTM-1 wykorzystują technologię usług SmartDefense™, która zapewnia najnowocześniejszą profilaktyczną ochronę dla infrastruktury bezpieczeństwa CheckPoint. Aktualizacje w czasie rzeczywistym, jakie zapewniają usługi SmartDefense™ pozwalają sprostać pojawiającym się nowym zagrożeniom i atakom.

BEZPIECZEŃSTWO KTÓREGO POTRZEBUJESZ

Sprawdzona kontrola aplikacji i ochrona przed atakami

UTM-1 zawiera najbardziej sprawdzoną w branży zaporę firewall. Posiada wbudowane mechanizmy zdolne do przeanalizowania setek predefiniowanych aplikacji, protokołów i usług. Obsługa wielu aplikacji i protokołów zapewnia szczegółową i ogólną kontrolę dostępu w sieci. Urządzenie UTM-1 zawiera system przeciwdziałania intruzom SmartDefense firmy CheckPoint, który chroni usługi kluczowe dla działania firmy takie, jak FTP, HTTP, POP3, i SMTP przed znanymi



OPIS PRODUKTU

Urządzenia UTM-1 oferują kompletny zestaw ściśle ze sobą zintegrowanych, sprawdzonych funkcji zabezpieczeń. W jego skład wchodzi zaporę firewall, system zapobiegania intruzom (IPS), antywirusowy, antyspyware, zaporę firewall dla aplikacji internetowych, zabezpieczenia ruchu VoIP, komunikatorów i aplikacji P2P, filtrowanie treści WWW, bezpieczna łączność pomiędzy odległymi lokalizacjami i zdalny dostęp.

WŁASNOŚCI PRODUKTU

- Najbardziej sprawdzona w branży zaporę firewall zabezpiecza setki aplikacji i protokołów
- Rozbudowany VPN IPsec zapewnia bezpieczną łączność pomiędzy odległymi lokalizacjami i zdalny dostęp
- Uniwersalny mechanizm zdalnego dostępu SSL bez konieczności instalowania dodatkowego sprzętu
- Zintegrowany system przeciwdziałania włamaniom (IPS)
- System antywirusowy na poziomie bramy dla kluczowych protokołów takich, jak FTP, HTTP, POP3 i SMTP
- Zaporę firewall dla aplikacji internetowych oraz zabezpieczenia antyspyware na poziomie bramy
- Intuicyjna konfiguracja sprzętu; narzędzia diagnostyczne i naprawcze
- W pełni scentralizowane zarządzanie obejmujące definiowanie polityk, aktualizacje, monitorowanie i tworzenie raportów
- Kluczowe aktualizacje bezpieczeństwa oraz porady dzięki zastosowaniu technologii usług SmartDefense™

KORZYŚCI Z ZASTOSOWANIA PRODUKTU

- Spokój o bezpieczeństwo dzięki sprawdzonym technologiom, którym zaufały firmy z listy Fortune 100
- Zabezpieczenie sieci, systemów i użytkowników przed wieloma typami zagrożeń w Internecie
- Zapewnienie poufności dzięki zabezpieczeniom zdalnego dostępu oraz komunikacji pomiędzy odległymi lokalizacjami
- Uproszczona instalacja zabezpieczeń i administracja
- Zabezpieczenia przed nowymi zagrożeniami dzięki technologii SmartDefense

NGX™

Platforma NGX dostarcza jednolitej architektury dla urządzeń CheckPoint.

i nieznanymi atakami. Obsługuje również nowe aplikacje, mające kluczowe znaczenie dla działania firm takie, jak protokół Voice over Internet Protocol (VoIP), z pełną obsługą standardów branżowych VoIP takich, jak H.323, MGCP i SIP.

Wreszcie, UTM-1 potrafi skutecznie blokować aplikacje niezwiązane z działalnością firmy takie, jak komunikatory oraz aplikacje współdzielenia plików P2P. Dzięki zastosowaniu wykrywania bazującego na sygnaturach protokołów, urządzenie UTM-1 zatrzymuje komunikację komunikatorów i aplikacji P2P nawet wtedy, kiedy wykorzystują one niestandardowe porty.

Zabezpieczenia przeciwko wirusom i robakom na poziomie bramy

Zabezpieczenia antywirusowe na poziomie bramy są w dalszym ciągu kluczowym komponentem skutecznego rozwiązania UTM i wprowadzają kluczową warstwę ochrony antywirusowej w komputerach typu desktop. Urządzenie UTM-1 zawiera mechanizmy antywirusowe, które w połączeniu z technologią SmartDefense tworzą zabezpieczenie na poziomie bramy przed oprogramowaniem spyware, wirusami i robakami. Mechanizm antywirusowy umożliwia skanowanie w czasie rzeczywistym wiadomości email (POP3 i SMTP), komunikacji FTP i ruchu WWW (HTTP) w poszukiwaniu zagrożeń ukrytych wewnątrz uprawnionej zawartości.

Antyspyware

Każde urządzenie UTM-1 zapewnia wielowarstwową ochronę na poziomie bramy zdolną do zwalczania zagrożeń i zakłóceń spowodowanych przez oprogramowanie spyware. Urządzenia UTM-1 wykorzystujące stale aktualizowany zbiór sygnatur antyspyware uzupełniają istniejące zabezpieczenia antyspyware komputerów desktop obecne w zabezpieczeniach punktów końcowych takich, jak rozwiązania Integrity™ firmy Check Point. Opcjonalne mechanizmy filtrowania ruchu WWW zapewniają jeszcze bardziej profilaktyczną ochronę dzięki blokowaniu witryn, o których wiadomo, że rozprowadzają oprogramowanie spyware.

Bezpieczeństwo ruchu WWW

Web Intelligence™ opcjonalny komponent urządzenia UTM-1 to zaporę firewall dla aplikacji internetowych, która zapewnia ochronę przed atakami z Internetu takimi jak: cross-site scripting, directory traversal oraz SQL injection. W skład Web Intelligence wchodzi oczekująca na opatentowanie rewolucyjna technologia Malicious Code Protector™ zdolna do wykrywania i blokowania ataków z wykorzystaniem przepelnienia bufora oraz złośliwych plików wykonywalnych, których celem są serwery WWW. Technologia Web Intelligence zatrzymuje zarówno znane, jak i nieznanne ataki, oferując profilaktyczną ochronę.

Filtrowanie ruchu WWW

Nieodpowiednie surfowanie w sieci WWW może stworzyć zagrożenie dla bezpieczeństwa firmy, a także zwiększa ryzyko poniesienia odpowiedzialności prawnej, obniżenia wydajności oraz naruszenia przepisów. Urządzenia UTM-1 integrują najlepsze w branży mechanizmy filtrowania ruchu WWW, których zasadniczą część stanowi rozbudowana baza danych kategorii zagrożeń i powiązanych z nimi adresów URL. Dzięki temu można zdefiniować politykę dopuszczalnego wykorzystania Internetu w firmie i zabezpieczyć się przed takimi zagrożeniami, jak oprogramowanie spyware i wirusy, a także nowymi niebezpieczeństwami związanymi z nieodpowiednią treścią stron WWW.

Prosta łączność pomiędzy odległymi lokalizacjami

Urządzenia UTM-1 upraszczają konfigurację sieci VPN pomiędzy odległymi lokalizacjami oraz zdalnego dostępu. Niepotrzebna jest ręczna konfiguracja tuneli VPN w trybie punkt-punkt. Zamiast tego parametry bezpieczeństwa dla całej sieci VPN włącznie ze zdalnym dostępem oraz łącznością pomiędzy odległymi lokalizacjami można zdefiniować w jednym kroku. Po skonfigurowaniu urządzeń UTM-1 sieci VPN są tworzone automatycznie dla wszystkich ośrodków i zdalnych użytkowników. Lokalizacje i użytkownicy dodawani do społeczności dziedziczą odpowiednie właściwości i mogą natychmiast nawiązywać bezpieczne sesje IPSec z pozostałymi użytkownikami.

Bezpieczny, uniwersalny zdalny dostęp

Urządzenia UTM-1 zapewniają pracownikom i partnerom biznesowym idealny sposób podłączania się do zaufanych sieci dzięki wykorzystaniu uniwersalności mechanizmów IPSec oraz zdalnego dostępu SSL oraz możliwości bezproblemowej pracy z różnymi klientami VPN. Każde urządzenie jest wyposażone w rozbudowane mechanizmy połączeń IPSec z możliwością dodania obsługi protokołu SSL za pomocą prostej aktualizacji licencji w postaci dodatku SSL Network Extender™ firmy Check Point. Firmy, które chcą zaimplementować silne uwierzytelnianie, mogą użyć technologii Check Point One-Click Certificates. Dzięki zintegrowanemu w urządzeniach UTM-1 modułowi Internal Certificate Authority, bramy UTM-1 i zdalni użytkownicy mogą otrzymywać cyfrowe certyfikaty X.509. Technologia One-Click Certificates zapewnia standardowość w branży, dwuskładnikowe uwierzytelnianie bez złożoności i kosztów związanych z zastosowaniem infrastruktury PKI.

PROSTOTA JAKIEJ OCZEKUJESZ

Szybka konfiguracja

Konfiguracja urządzeń UTM-1 zajmuje mniej niż 10 minut. Dzięki temu instalacja urządzeń w firmach o ograniczonych zasobach IT jest niezwykle prosta. Dzięki użyciu dołączonego do urządzeń Kreatora pierwszej konfiguracji, osoby bez wiedzy technicznej mogą z łatwością przeprowadzić wstępną instalację i konfigurację urządzeń. Po podłączeniu do sieci i włączeniu urządzenia, kreator przeprowadza użytkowników przez proces konfiguracji i przygotowuje urządzenie do zarządzania za pomocą mechanizmów SmartCenter™. Po skonfigurowaniu urządzeniami UTM-1 można zarządzać i aktualizować je zdalnie wykorzystując standardowe mechanizmy zarządzania firmy Check Point.



Dzięki kreatorowi pierwszej konfiguracji, konfiguracja urządzeń UTM-1 jest bardzo prosta

Zintegrowane zarządzanie SmartCenter

Urządzenia UTM-1 są zintegrowane z technologią SmartCenter, która umożliwia centralne zarządzanie wieloma urządzeniami i innymi produktami Check Point z poziomu pojedynczej konsoli. Zapisane są w niej centralnie i z tego miejsca rozpowszechniane polityki bezpieczeństwa dla całej infrastruktury, co eliminuje konieczność oddzielnego utrzymywania ich dla każdej witryny i bramy. Takie rozwiązanie zmniejsza obciążenie administratorów i minimalizuje błędy oraz zapewnia spójność konfiguracji w całej sieci.

Dzięki intuicyjnej technologii SmartDashboard™, administratorzy definiują i zarządzają elementami polityki bezpieczeństwa: zabezpieczeniami firewall, translacją adresów sieciowych, jakością usług (*Quality of Service – QoS*), bezpieczeństwem klientów VPN oraz sieciami VPN. Architektura SMART firmy Check Point pomaga zarządzać zmianami w środowisku dzięki mechanizmom kontroli wersji obiektów zabezpieczeń oraz polityk do celów audytu lub szybkiego przywracania ich poprzednich wersji (ang. *Roll-back*).

Scentralizowane, automatyczne aktualizacje

W celu utrzymania profilaktycznego środowiska zabezpieczeń oraz zapewnienia ochrony sieci przed nowymi atakami, opcjonalne usługi SmartDefense zapewniają automatyczne aktualizacje mechanizmów obrony, polityk oraz innych elementów zabezpieczeń. Aktualizacje mogą być pobierane automatycznie i rozprowadzane do zdalnych lokalizacji w ustalonych odstępach czasu.

Monitorowanie w czasie rzeczywistym i szczegółowe raporty Urządzenia UTM-1 są wyposażone w zestaw narzędzi do monitorowania i tworzenia raportów. Zapewniają one kompletny, szczegółowy wgląd w stan zabezpieczeń.

Narzędzia administracyjne klasy korporacyjnej takie, jak technologie SmartView Monitor™ oraz SmartViewTracker™ umożliwiają kompleksowe rejestrowanie, monitorowanie w czasie rzeczywistym oraz tworzenie szczegółowych raportów z możliwością definiowania własnych kryteriów wyszukiwania i przedziałów czasowych.

Wbudowane narzędzie Express Reports zapewnia możliwość dostosowywania raportów w różnych formatach, oferując cenny wgląd w trendy zabezpieczeń oraz rozwój sytuacji w czasie.

The screenshot displays the SmartView Monitor application window. At the top, there is a menu bar with options like 'File', 'Gateways', 'Query', 'View', 'Tools', 'Window', and 'Help'. Below the menu is a toolbar with various icons. The main area is divided into a left-hand navigation pane and a central content area.

The left-hand pane shows a tree view under 'All' with categories such as 'Custom', 'Gateways Status', 'Firewalls', 'VPNs', 'VPN-1 UTM Edge', 'Traffic', 'System Counters', 'Tunnels', 'Remote Users', and 'Cooperative Enforcement'. The 'Gateways Status' category is selected, showing a table of gateway information.

Gateway Name	IP Address	Status	Average CPU	Active Virtual Memory	Disk Free %	Version
Corporate-Cluster-1-member-A	143.100.76.1	OK	5%	0	0	NGX (R65)
Corporate-Cluster-1-member-B	143.100.76.2	OK	24%	0	0	NGX (R65)
Corporate-Cluster-2-member-A	143.100.80.1	OK	13%	0	0	NGX (R65)
Corporate-Cluster-2-member-B	143.100.80.2	OK	52%	0	0	NGX (R65)
Remote-2-windows-domain-controller	10.0.2.10	OK	36%	0	0	NGX (R65)
Management	143.29.47.78	OK	2%	0	0	NGX (R65)
Remote-1-web-server	192.168.2.2	OK	11%	0	0	NGX (R65)
Corporate-WA-proxy-server	172.16.2.3	OK	15%	0	0	NGX (R65)
Corporate-internal-terminal-server	172.16.1.10	OK	73%	0	0	NGX (R65)

The central content area shows detailed information for the selected gateway 'Corporate-Cluster-1-member-A'. It includes a green checkmark icon, the IP address '143.100.76.1', the version 'NGX (R65)', and the operating system 'SecurePlatform'. Below this, there are three sections with green checkmarks: 'Firewall' (Security Policy: Standard, Installed On: 01.03.04), 'ClusterXL' (Working mode: High Availability, Member state: Up), and 'VPN' (Gateway to Gateway Tunnels: 61). Each section has a 'More...' link.

SmartView Monitor zapewnia wgląd w czasie rzeczywistym w status urządzenia, ruch sieciowy oraz status tuneli VPN.

Odtwarzanie systemu i kopie zapasowe

Każde urządzenie UTM-1 jest wyposażone w podłączany przez port USB token, który ułatwia odtwarzanie systemu. W przypadku błędnej konfiguracji lub jeśli urządzenie nie odpowiada, można wykorzystać token do odtworzenia konfiguracji urządzenia UTM-1 do ustawień fabrycznych.

WYDAJNOŚĆ I DOSTĘPNOŚĆ

Urządzenia UTM-1 są wyposażone w kluczowe własności wysokiej dostępności i mechanizmy zapewnienia jakości usług. Dzięki nim zabezpieczenia dotrzymują tempa sieci i aplikacjom istotnym dla działania firmy.

Budowa klastrów oraz funkcje pracy w warunkach awarii (failover)

Technologia ClusterXL® opcjonalny komponent urządzeń UTM-1 dostarcza funkcji równoważenia obciążenia, dzięki czemu poprawia wydajność i skalowalność rozwiązania.

Aby zapewnić ciągłość działania sieci i jej bezpieczeństwo, można połączyć wiele urządzeń UTM-1 w klastry.

Jeśli podstawowa brama stanie się niedostępna, wszystkie połączenia są w przezroczysty dla użytkownika sposób przekierowywane do pozostałych urządzeń w klastrze. Dodanie do klastra dodatkowych bram pozwala na niemal liniowy wzrost wydajności. Interfejs HA pozwala na kierowanie ruchu do redundantnego interfejsu bądź łącza dostawcy Internetu w przypadku, gdy podstawowy interfejs jest niedostępny. W warunkach awarii przez cały czas utrzymywane są bieżące połączenia.

Jakość usług

FloodGate-1® opcjonalny moduł urządzenia UTM-1 kształtuje ruch VPN dzięki przydzielaniu priorytetów do aplikacji o kluczowym znaczeniu oraz użytkowników. Pozwala on na zoptymalizowanie wydajności, umożliwiając klientom przeniesienie ruchu biznesowego z drogich linii dzierżawionych na internetowe sieci VPN.

	UTM-1 450	UTM-1 1050	UTM-1 2050
Przepustowość zapory firewall	400 Mb/sek	1 Gb/sek	2 Gb/sek
Przepustowość VPN	190 Mb/sek	250 Mb/sek	400 Mb/sek
Liczba jednoczesnych sesji	500 000	1.2 miliona	2 miliony
Liczba obsługiwanych użytkowników/liczba zalecana	Nieograniczona/250	Nieograniczona/500	Nieograniczona/1000
Liczba sieci VLAN	256	256	256
Pamięć zewnętrzna	80 GB	80 GB	80 GB
Specyfikacja fizyczna			
Obudowa	1U do zamontowania w szafie	1U do zamontowania w szafie	1U do zamontowania w szafie
Wymiary (cale)	1.71 (H) x 16.77 (W) x 14.31 (D)	1.71 (H) x 16.77 (W) x 17 (D)	1.71 (H) x 16.77 (W) x 17 (D)
Wymiary (milimetry)	43.5 mm (H) x 426 mm (W) x 365 mm (D)	43.5 mm (H) x 426 mm (W) x 431.8 mm (D)	43.5 mm (H) x 426 mm (W) x 431.8 mm (D)
Waga	2.2 kg (4.85 lbs)	2.3 kg (5 lbs)	2.3 kg (5 lbs)
Liczba interfejsów 10/100	-	4	4
Liczba interfejsów 10/100/1000	4	4	4
Środowisko pracy	Temperatura: 5°-40°C (41°-104°F)		
	Wilgotność: 10%-90% bez kondensacji		
	Wysokość: 3.048 m (10 ft.)		
Zasilanie	100-240 VAC, 250 W	100-240 VAC, 250 W	100-240 VAC, 250 W
Zgodność z przepisami	UL 60950; FCC Część 15, podrozdział B, klasa A; EN 55024; EN 55022; VCCI V-3; AS/NZS 3548:1995; CNS 13438 Klasa A (testy pomysłne, oczekuje na zatwierdzenie); KN22, KN61000-4, TTA; IC-950; ROHS		
Gwarancja na sprzęt	2 lata	2 lata	2 lata

2003-2007 Check Point Software Technologies Ltd. Wszystkie prawa zastrzeżone. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo są zastrzeżonymi znakami handlowymi lub zarejestrowanymi znakami handlowymi firmy Check Point Software Technologies Ltd. bądź jej partnerów. ZoneAlarm jest znakiem należącym do firmy Check Point Software Technologies, Inc. Company. Wszystkie inne nazwy produktów wymienione w tym dokumencie są znakami handlowymi bądź zarejestrowanymi znakami handlowymi należącymi do ich prawowitych właścicieli. Produkty opisane w tym dokumencie są chronione patentami w USA nr. 5 606 668, 5 835 726, 6 496 935, 6 873 988 oraz 6 850 943. Mogą również być chronione innymi patentami w USA, patentami w innych krajach lub mogą oczekiwać na opatentowanie.
28 lutego 2007 P/N 502439

Dystrybucja w Polsce:



CLICO Sp. z o.o.
30-063 Kraków, Al. 3-go Maja 7
tel. 012 632-51-66
tel. 012 292-75-22 ... 25
fax 012 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-555 Katowice, ul. Rolna 43
tel. 032 203-92-35
tel. 032 609-80-50
tel. 032 609-80-51
fax 032 203-92-24
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
03-738 Warszawa, ul. Kijowska 1
tel. 022 518-02-70...75
fax 022 518-02-73
e-mail: warszawa@clico.pl

© 2007 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.

Centrala międzynarodowa
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

Oddział w Polsce:
Check Point Software Technologies (Poland) Sp. z o.o.
Warsaw Financial Centre
ul. Emilii Plater 53 (11 piętro)
00-113 Warszawa
tel: +48 0 22 5286806
Fax: +48 022 5286837
e-mail: info_cp@checkpoint.com



Check Point®
SOFTWARE TECHNOLOGIES LTD.