CLOUDORAMA

OPIS USŁUGI

Firewall VM

Prywatna zapora sieciowa

Dostawca usługi	**Cloudorama**
Dystrybutor	**Cloudorama**
Wersja dokumentu	**Stan: 05/2026**
Przeznaczenie	**Opis usługi dla Klientów**

Spis treści

1 Opis produktu

Cloudorama udostępnia Klientowi – o ile jest to ujęte w pakiecie podstawowym lub zostało zamówione – prywatną zaporę sieciową w postaci maszyny wirtualnej (Firewall VM). Firewall VM łączy publiczny internet z siecią prywatną, która jest dedykowana Klientowi jako wydzielony segment VLAN. Klient używa w swojej sieci prywatnej wyłącznie prywatnych adresów IP zgodnych z RFC 1918. Głównym zadaniem Firewall VM jest ochrona sieci Klienta przy użyciu różnych mechanizmów.

2 Elementy usługi

2.1 Translacja Adresów Sieciowych (NAT)

Usługa ta służy do przekształcania prywatnych adresów IP sieci klienta na publiczne adresy IP internetu (Source NAT) oraz do przekształcania publicznych adresów IP obecnych na zewnętrznym interfejsie Firewall VM na prywatne adresy IP w sieci klienta (Destination NAT). Mechanizm translacji oparty jest na fragmentach standardów RFC 2663, 2766 i 3022.

2.2 Filtrowanie pakietów (z inspekcją stanową SPI)

W celu kontrolowania, które publiczne adresy IP mogą komunikować się z adresami IP sieci klienta (wymieniać pakiety IPv4), dostępny jest filtr pakietów. Do wyboru reguły dostępne są następujące kryteria decyzyjne:

- Źródłowy adres IPv4 komunikacji
- Docelowy adres IPv4 komunikacji
- Używany protokół transportowy (TCP, UDP, ESP i ICMP)

W przypadku protokołów transportowych TCP i UDP możliwe jest dodatkowo uwzględnienie portów źródłowych i docelowych używanych w tych protokołach. Zapora obsługuje do 500 takich reguł na jedną instancję Firewall VM. Zestaw reguł przetwarzany jest od wiersza 1 w dół. Gdy reguła zostaje dopasowana, wykonywana jest jej akcja i żadne kolejne reguły nie są brane pod uwagę dla tego pakietu.

Dostępne akcje:

- "Accept" – pakiet i powiązana z nim komunikacja zostają dopuszczone
- "Drop" – pakiet zostaje odrzucony (zapora nie wysyła odpowiedzi do nadawcy)
- "Reject" – pakiet zostaje odrzucony z odpowiedzią w postaci pakietu ICMP "Destination Unknown"
- "Stateless" – połączenia są dopuszczane niezależnie od stanu (zalecane dla połączeń VoIP)
- "QoS" – umożliwia ograniczenie przepustowości dla danej reguły

2.3 Reguły niejawne

W ramach Firewall VM istnieją tzw. reguły niejawne (implicit rules). Reguły te zezwalają na ruch sieciowy określonych protokołów lub go zabraniają. Reguły niejawne mogą być przez klienta wyłącznie włączane lub wyłączane, nie mogą natomiast być modyfikowane.

2.3.1 Funkcja VPN – OpenVPN

W celu zapewnienia klientowi szyfrowanego dostępu do jego urządzeń (w tym do Firewall VM) w sieci klienta, zapora udostępnia połączenie VPN.

Połączenie to oparte jest na oprogramowaniu OpenVPN i w ustawieniu domyślnym wykorzystuje protokół UDP do transportu całego połączenia (sterowanie i dane).

Aby klient mógł nawiązać połączenie VPN z Firewall VM, na używanym systemie operacyjnym musi być zainstalowany klient obsługujący OpenVPN. Odpowiedni plik konfiguracyjny oraz dane dostępowe (nazwa użytkownika i hasło) są umieszczane w panelu Cloudorama po zakończeniu procesu zamawiania.

Klient musi ponadto zapewnić, że dany komputer ma domyślnie nieograniczony dostęp do protokołu UDP – z dowolnego portu źródłowego na port docelowy 1194 – do momentu dotarcia do Firewall VM sieci klienta.

Administrator może konfigurować i używać dodatkowych kont OpenVPN. Połączenie to jest odpowiednie zarówno dla pojedynczych stanowisk roboczych, jak i dla tzw. sprzężenia LAN-LAN. Jako punkty końcowe sprzężenia LAN-LAN dopuszczone są zapory sieciowe firmy Wortmann AG oraz Securepoint. Zapory innych producentów muszą zostać przetestowane przez klienta pod kątem kompatybilności z Firewall VM sieci klienta na jego własny koszt i ryzyko.

2.3.2 Funkcja VPN – IPSec VPN

Do podłączania urządzeń końcowych oraz sprzężenia LAN-LAN dostępny jest również protokół VPN IPSec.

Do podłączania urządzeń końcowych zalecamy korzystanie z OpenVPN.

Jako punkty końcowe sprzężenia LAN-LAN z użyciem IPSec dopuszczone są zapory sieciowe firmy Wortmann AG oraz Securepoint.

2.3.3 Administracja / Odpowiedzialność administracyjna

Administracja zapory sieciowej jest realizowana przez Cloudorama. Błędna konfiguracja może np. odciąć Klienta od administrowania własną siecią. Na życzenie Klienta administracja zapory może zostać przekazana Klientowi jako opcja dodatkowa (zob. pkt 3.1.2).

2.4 Rozszerzenia/zmiany usług

Rozszerzanie i zmiana usług odbywa się na podstawie zgłoszenia Klienta.

Zmiany przeprowadzane są w terminie indywidualnie uzgodnionym z klientem i zależą od czasu realizacji oraz dostępności wymaganych komponentów.

Zmiany i rozszerzenia mogą prowadzić do krótkotrwałej niedostępności systemu lub jego restartu. Planowany czas przestoju jest wyłączony z obliczania dostępności produktu głównego i jest realizowany – za zgodą klienta – przede wszystkim w wyznaczonych oknach serwisowych.

2.5 Usługi jednorazowe

Usługi jednorazowe mogą być zlecane kontaktując się z Cloudorama. Usługi te są rozliczane w formie ryczałtu zgodnie z aktualnym cennikiem.

2.6 Bezpieczne usuwanie danych

Po zakończeniu zlecenia jednostkowego, po 14 dniach automatycznie usuwane są dyski twarde serwera, przypisane woluminy storage oraz odpowiednie dyski użytkownika. Usunięcie danych użytkownika następuje zgodnie ze standardem DOD 5220.22-M. Ewentualne dane kopii zapasowych są również usuwane. Po pomyślnym zakończeniu procesu usuwania klient otrzymuje potwierdzenie usunięcia.

Po zakończeniu umowy ramowej dostęp do zdalnego połączenia z centrum danych zostaje dezaktywowany. Udostępniony sprzęt, np. Connector, musi zostać zwrócony do Cloudorama w ciągu 14 dni.

3 Opcje dodatkowe

3.1 Zarządzanie zaporą sieciową

Zarządzanie i administrowanie Firewall VM jest realizowane przez Cloudorama. Na życzenie Klienta, posiadającego własny zespół IT, administracja zapory może zostać przekazana Klientowi.

3.1.1 Konfiguracja wstępna

Firewall VM dostarczany jest z wstępnie skonfigurowanymi ustawieniami, a następnie przez zespół Cloudorama dostosowywana do konfiguracji uzgodnionej z klientem. W tym celu klient otrzymuje kwestionariusz, który musi wypełnić i zwrócić. Konfigurowalne elementy Firewall VM odpowiadają możliwościom wynikającym z niniejszego opisu usługi. Usługi nieuwzględnione w opisie mogą być dodatkowo skonfigurowane odpłatnie po indywidualnym rozpatrzeniu. Nie istnieje prawo do konfiguracji wykraczających poza niniejszy opis usługi.

Konfiguracja wstępna ograniczona jest do 40 obiektów sieciowych i 40 reguł filtrowania portów, a także konfiguracji jednego sprzężenia IPSEC LAN-LAN oraz utworzenia trzech dostępów OpenVPN dla trybu road-warrior. Dodatkowe konfiguracje dostępne są za dopłatą. Po pomyślnym przejściu testu zapora jest zarządzana przez Cloudorama, wobec czego obowiązują warunki opisane w pkt 3.1.2.

3.1.2 Zapora w pełni zarządzana (Full Managed Firewall)

Całość konfiguracji i zarządzania Firewall VM jest wykonywana przez Cloudorama i jej podwykonawców. Po udostępnieniu Firewall VM jest ona konfigurowana zgodnie z danymi uzgodnionymi z klientem. W celu przeprowadzenia konfiguracji klient otrzymuje kwestionariusz, który musi wypełnić i zwrócić do Cloudorama.

Opcja Full Managed Firewall może być zamówiona wyłącznie w połączeniu z konfiguracją wstępną. Konfiguracja wstępna realizowana jest zgodnie z opisem w pkt 3.1.1.

W ramach zmian (change requests) w trakcie eksploatacji klient dysponuje kontyngentem pojedynczych działań. Klient może zlecić:

- 40 obiektów sieciowych
- 40 reguł filtrowania portów
- jedno sprzężenie IPSEC LAN-LAN
- do 3 dostępów OpenVPN dla trybu road-warrior

– do nowej konfiguracji lub modyfikacji.

Dodatkowe konfiguracje dostępne są za dopłatą. Kontyngent jest odnawiany co dwanaście miesięcy do wartości wskazanych powyżej. Nieużyte kontyngenty z poprzedniego okresu przepadają.

3.2 Dodatkowe funkcje ochrony

3.2.1 Ochrona internetowa

Ochrona internetowa łączy funkcje pakietu filtrowania treści oraz pakietu antywirusowego i może być opcjonalnie dodana za opłatą.

Pakiet filtrowania treści służy do analizy i kontroli strumieni danych HTTP i HTTPS wychodzących z sieci klienta do publicznego internetu. Ruch HTTP i HTTPS może być automatycznie (transparentnie) wyodrębniany z ruchu sieciowego lub serwer proxy HTTP może być na stałe skonfigurowany w oprogramowaniu wewnątrz sieci klienta.

Pakiet filtrowania treści oferuje następujące funkcje:

- Kontrola dostępu na podstawie użytkowników (wyłącznie przy aktywnym uwierzytelnianiu), obiektów sieciowych i grup sieciowych
- Zezwalanie/blokowanie poszczególnych stron internetowych
- Zezwalanie/blokowanie kategorii stron internetowych
- Zezwolenia mają zawsze pierwszeństwo przed blokadami

W celu analizy przynależności adresu URL do danej kategorii jest on przekazywany do producenta oprogramowania Firewall VM.

W ramach pakietu antywirusowego serwer proxy HTTP sprawdza przekierowywany ruch pod kątem wirusów; dostępny jest wybór spośród dwóch skanerów antywirusowych. Pakiet antywirusowy nie zastępuje oprogramowania antywirusowego na systemach serwerowych lub klienckich.

3.2.2 Ochrona poczty e-mail

Ochrona poczty e-mail łączy funkcje pakietu antyspamowego oraz pakietu antywirusowego i może być opcjonalnie dodana za opłatą.

Pakiet antyspamowy umożliwia klientowi oczyszczenie strumieni danych SMTP z niechcianych wiadomości e-mail. W tym celu konieczne jest, aby klient kierował filtrowane dane e-mail za pomocą protokołu SMTP przez przekaźnik pocztowy (mail relay) zapory. Klient może tu określić, dla jakich domen przyjmuje wiadomości e-mail i gdzie mają być one przekazywane po filtracji.

Do ochrony przed spamem Firewall VM dysponuje następującymi mechanizmami:

3.2.2.1 Pauza powitalna (Greeting Pause)

Na początku komunikacji Firewall VM wprowadza pauzę w przewidzianym przez SMTP powitaniu (greeting). Jeśli w tym czasie strona zdalna prześle dalsze dane, połączenie zostaje przerwane. Funkcja ta może być włączana i wyłączana.

3.2.2.2 Greylisting

Mechanizm greylisting polega na przyjmowaniu wiadomości e-mail przez SMTP wyłącznie wtedy, gdy nadawca przesłał już wcześniej wiadomość do odbiorcy z tego samego serwera nadawczego. Jeśli serwer pocztowy po raz pierwszy wysyła wiadomość do odbiorcy klienta, połączenie to jest odrzucane z tymczasowym błędem.

Funkcja greylisting nie jest zgodna ze standardem RFC 2821 (SMTP) i może powodować opóźnienia w dostarczaniu również pożądanych wiadomości e-mail.

3.2.2.3 Procedura identyfikacji wiadomości

Na podstawie treści sprawdzanej wiadomości e-mail generowany jest identyfikator wiadomości (Message ID). Jest on przekazywany do centralnej bazy danych producenta, a Firewall VM otrzymuje z powrotem status danej wiadomości. Status wiadomości może brzmieć:

- "Clean" – wiadomość nie budzi podejrzeń
- "Probably Spam" – wiadomość jest prawdopodobnie niechciana
- "Spam" – wiadomość jest spamem

Skuteczność wykrywania spamu przy aktywacji wszystkich funkcji wynosi co najmniej 98% w skali roku. Wskaźnik błędów, tj. klasyfikowanie pożądanych wiadomości jako spam, wynosi poniżej 1% w skali roku.

Przy aktywowanym pakiecie antywirusowym Firewall VM sprawdza również przekazywane wiadomości e-mail pod kątem wirusów; w tym celu używane są kolejno oba wbudowane skanery antywirusowe.

4 Wymagania i obowiązki współpracy

Warunkiem korzystania z Firewall VM jest użytkowanie produktu z jednego z następujących obszarów:

- Cloudorama Serwer dedykowany
- Cloudorama VPS/VDI
- Istnieje aktywne połączenie z internetem (mogą z tego wynikać dodatkowe koszty).
- Klient ma dostęp do panelu Cloudorama.
- Klient zapewnia kompetentnego i upoważnionego do podejmowania decyzji przedstawiciela kontaktowego.
- Klient aktywnie zgłasza pracowników, których dostępy do panelu Cloudorama nie będą już w przyszłości potrzebne ani używane
- Klient akceptuje usuwanie zainfekowanych plików w ramach zasobów danych.
- Klient ponosi odpowiedzialność za jakość danych udostępnionych danych osobowych i organizacyjnych.
- Klient zapewnia, że numery telefonów użytkowników, w tym numery wewnętrzne, są poprawnie wprowadzone.

Jeśli jeden z opisanych tutaj warunków nie jest spełniony, Cloudorama nie jest zobowiązana do świadczenia opisanej usługi z uzgodnionymi poziomami serwisu.

Obowiązki współpracy są co do zasady realizowane w jakości umożliwiającej Cloudorama wywiązanie się ze zobowiązań umownych bez dodatkowego nakładu pracy. Opóźnienia w świadczeniu usług i/lub naruszenia uzgodnionych poziomów serwisu wynikające z niewywiązania się przez klienta z obowiązków współpracy lub niezawinione przez Cloudorama nie obciążają Cloudorama.

5 Ceny

Aktualne ceny usług dostępne są w cenniku Cloudorama lub na życzenie u opiekuna handlowego.

6 Czas trwania umowy

Rozliczenie rozpoczyna się z chwilą zamówienia usługi w Panelu Klienta Cloudorama lub z chwilą zawarcia Umowy Wdrożeniowej, której elementem jest dana usługa. Nie obowiązuje minimalny czas trwania umowy. Umowa przedłuża się automatycznie o jeden miesiąc, o ile nie zostanie wypowiedziana z zachowaniem 4-tygodniowego okresu wypowiedzenia przed upływem minimalnego czasu trwania umowy lub przed końcem okresu przedłużenia.

7 Rozliczenia

Rozliczenie rozpoczyna się z chwilą zamówienia usługi w Panelu Klienta Cloudorama lub z chwilą zawarcia Umowy Wdrożeniowej, której elementem jest dana usługa. Okres rozliczeniowy jest miesięczny. Rozpoczęte miesiące są rozliczane jako pełne miesiące. Fakturowanie odbywa się z góry za dany okres rozliczeniowy. W przypadku przekroczenia zamówionego zużycia, wyrównanie jest fakturowane w następnym miesiącu.

8 Pakiet serwisowy

Partner technologiczny Cloudorama prowadzi Centrum Zarządzania Systemami (Systems Management Center– SMC), w którym realizowane są wszystkie zadania codziennej eksploatacji. SMC monitoruje systemy przez 365 dni w roku, 24 godziny na dobę (24/7). Obsługa i administracja systemów odbywa się od poniedziałku do piątku w godzinach 8:00–18:00 (z wyłączeniem świąt i dni wolnych od pracy).

8.1 Godziny serwisu i dane kontaktowe

Przyjmowanie zgłoszeń odbywa się całą dobę, 7 dni w tygodniu, również w niedziele i święta. Zgłoszenia można składać przez e-mail lub przez system ticketowy.

8.2 Przyjmowanie zgłoszeń

Punkt przyjmowania zgłoszeń przyjmuje żądania telefonicznie lub e-mailem w uzgodnionych godzinach serwisu. Przy zgłoszeniu należy podać numer klienta, numer pakietu i identyfikator systemu serwera. Na podstawie podanych danych pracownik Service Desk identyfikuje klienta przy użyciu danych kontaktowych zarejestrowanych w systemie i przeprowadza weryfikację uprawnienia do danej usługi.

Każdy e-mail lub rozmowa telefoniczna jest automatycznie rejestrowana w bazie danych jako żądanie serwisowe. Każde przychodzące zgłoszenie jest tworzone w systemie ticketowym jako zgłoszenie z unikalnym numerem (ID). Numer zgłoszenia jest przekazywany zgłaszającemu jako numer referencyjny.

W zależności od klasyfikacji jako Change Request lub Incydent (przerwa w usłudze/usterka techniczna) stosowane są dalsze kroki procesowe.

8.3 Zarządzanie incydentami (przerwa w usłudze / usterka techniczna)

W przypadku incydentu pracownik Service Desk przeprowadza diagnozę techniczną i stara się niezwłocznie znaleźć rozwiązanie przy użyciu bazy wiedzy. Pomyślne rozwiązanie oraz podjęte kroki zaradcze są dokumentowane, a po usunięciu usterki incydent zostaje zamknięty. Klient jest informowany o usunięciu usterki. Jeśli natychmiastowe rozwiązanie nie jest możliwe, wszystkie dotychczasowe działania są dokumentowane, a sprawa jest przekazywana do instancji wyższego poziomu (2nd Level Support lub Centrum Zarządzania Systemami).

8.4 Wsparcie drugiego poziomu (2nd Level Support)

Wsparcie drugiego poziomu obsługuje incydenty i pytania dotyczące uzgodnionego zakresu produktu, których nie udało się rozwiązać na pierwszym poziomie wsparcia. Świadczenia 2nd Level Support obejmują:

- Obsługę żądań z Service Desk przez specjalistów Partnera Technologicznego, o ile nie są obsługiwane przez innych dostawców usług.
- Ewentualne odtworzenie sytuacji błędu i przeprowadzenie analiz incydentów.
- Ewentualne telefoniczne wsparcie klienta w incydentach i pytaniach dotyczących obsługi w zakresie uzgodnionego produktu.
- Przekazywanie nierozwiązanych żądań do instancji wyższego poziomu.

9 SLA

Obowiązują umowy SLA produktu głównego.

9.1 Poziom usług

Zawarcie Umów o Poziomie Usług (Service Level Agreements – SLA) stanowi umowną podstawę między zleceniodawcą a Cloudorama w zakresie świadczenia usługi Firewall.

Parametr	Wartość
Eksploatacja serwisu	24/7
Obsługiwany czas serwisu	pon.–pt. 8:00–20:00 CET
Dostępność poziomu usług	Infrastruktura centrum danych
Planowane okna serwisowe	pon.–pt.: 18:30–22:30 / sob.: 06:00–10:00

Pakiet Firewall uznaje się za udostępniony i gotowy do pracy, gdy Cloudorama przekazała klientowi informacje niezbędne do uruchomienia i konfiguracji. Zgodnie z zamówieniem w tym momencie przekazywane są ewentualne dane uwierzytelniające.

Dostępność zapory sieciowej jest uznawana za zapewnioną, gdy odpowiednia infrastruktura serwerowa jest osiągalna z sieci Cloudorama lub gdy wolumin działa. Pomiar dostępności odbywa się na podstawie monitorowania wydajności i statusu systemów serwerowych przez system zarządzania Cloudorama.

Cloudorama może przeprowadzać zmiany w oprogramowaniu i/lub systemach sprzętowych poza oknami serwisowymi, o ile nie prowadzi to do naruszenia uzgodnionej dostępności.

10 Pozostałe postanowienia

Ogólne Warunki Współpracy Cloudorama, Regulamin Świadczenia usług Drogą elektroniczną, aktualny cennik oraz opisy usług.