РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2005 131 831** (13) **A**

(51) МПК
G06N 1/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2005131831/09, 13.10.2005**

(30) Конвенционный приоритет:
14.10.2004 US 60/618,139
14.02.2005 US 11/056,276

(43) Дата публикации заявки: **20.04.2007 Бюл. № 11**

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

(72) Автор(ы):
СВЕНДЕР Брайан Д. (US),
БЛЭК Кристофер Дж. (US),
ЙОХАНССОН Йеспер М. (US),
МЕРТИ Картик Н. (US),
МЭЙФИЛД Пол Дж. (US)

(54) СИСТЕМА И СПОСОБЫ ДЛЯ ОБЕСПЕЧЕНИЯ СЕТЕВОГО КАРАНТИНА С ИСПОЛЬЗОВАНИЕМ IPsec

(57) Формула изобретения

1. Способ, позволяющий хосту обеспечивать избирательную сетевую изоляцию в сети с использованием протокола безопасности IP (IPsec), содержащий этапы, на которых принимают пакет "обмена ключами Интернета" (IKE), включающий в себя утверждение здоровья клиента от клиента, проверяют утверждение здоровья клиента, отправляют клиенту утверждение здоровья хоста, если сертификат здоровья клиента верен, и отказывают клиенту в доступе к хосту, если сертификат здоровья клиента неверен.

2. Способ по п.1, в котором сертификат здоровья указывает, что владелец сертификата отвечает политикам безопасности сети.

3. Способ по п.1, который также содержит этап, на котором осуществляют связь с клиентом посредством связи IPsec, если сертификат здоровья клиента верен.

4. Способ по п.1, в котором сертификат здоровья представляет собой сертификат X509.

5. Способ по п.1, в котором сертификат здоровья представляет собой билет Кербероса.

6. Способ по п.1, в котором сертификат здоровья представляет собой жетон WS-Security.

7. Компьютерно-считываемый носитель, на котором хранятся компьютерно-выполняемые команды для осуществления способа по п.1.

8. Способ, позволяющий хосту приобретать сертификат здоровья, содержащий этапы, на которых отправляют одно или более утверждений о здоровье на сервер сертификатов здоровья, принимают ответ на утверждение о здоровье от сервера сертификатов здоровья, и, если сервер сертификатов здоровья признал, по меньшей мере, одно утверждение о здоровье, принимают сертификат здоровья и конфигурируют хост для реализации политики IPsec, которая требует от клиента сертификат здоровья клиента, прежде чем предоставить клиенту доступ к хосту.

9. Способ по п.8, в котором, если, по меньшей мере, одно утверждение о здоровье не признано, то, по меньшей мере, один ответ на утверждение о здоровье указывает, что хост не согласуется с сетевыми политиками безопасности.

10. Способ по п.8, в котором сертификат здоровья представляет собой сертификат X509.

RU 2005131831 A

RU 2005131831 A

11. Способ по п.8, в котором сертификат здоровья представляет собой билет Кербероса.

12. Способ по п.8, в котором сертификат здоровья представляет собой жетон WS-Security.

13. Компьютерно-считываемый носитель, на котором хранятся компьютерно-выполняемые команды для осуществления способа по п.8.

14. Компьютерная сеть, реализующая модель сетевой изоляции, содержащая первую группу компьютеров, в которой каждый компьютер имеет сертификат здоровья и осуществляет связь только с компьютерами, которые также имеют верный сертификат здоровья, вторую группу компьютеров, в которой каждый компьютер имеет сертификат здоровья и осуществляет связь со всеми остальными компьютерами в сети, и третью группу компьютеров, в которой ни один из компьютеров не имеет сертификата здоровья и осуществляет связь со всеми остальными компьютерами в сети.

15. Сеть по п.14, в которой связь между компьютерами в первой группе и между компьютерами первой группы и компьютерами второй группы осуществляется с использованием IPsec.

16. Сеть по п.14, в которой сертификат здоровья представляет собой сертификат X509.

17. Сеть по п.14, в которой сертификат здоровья представляет собой билет Кербероса.

18. Сеть по п.14, в которой сертификат здоровья представляет собой жетон WS-Security.

19. Сеть по п.14, в которой сертификат здоровья указывает, что владелец сертификата отвечает политикам безопасности сети.

20. Сеть по п.14, в которой компьютеры в первой группе могут инициировать связь с компьютерами в третьей группе, но компьютеры в третьей группе не могут инициировать связь с компьютерами в первой группе.

RU 2005131831 A

RU 2005131831 A