(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104079570 B
(45)授权公告日 2017.09.22

(21)申请号 201410294716.7

(22)申请日 2014.06.27

(65)同一申请的已公布的文献号
申请公布号 CN 104079570 A

(43)申请公布日 2014.10.01

(73)专利权人 东湖软件产业股份有限公司
地址 430070 湖北省武汉市武昌区关山一路光谷软件园A8栋3楼

(72)发明人 刘毅 周艳钢 余发江 肖霄 冯振新

(74)专利代理机构 武汉凌达知识产权事务所（特殊普通合伙）42221
代理人 宋国荣

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 102970293 A,2013.03.13,
CN 101242266 A,2008.08.13,
CN 101159640 A,2008.04.09,
CN 101350721 A,2009.01.21,
CN 101136928 A,2008.03.05,
EP 2211570 A1,2010.07.28,
CN 101242268 A,2008.08.13,
CN 1848722 A,2006.10.18,

审查员 曾珍

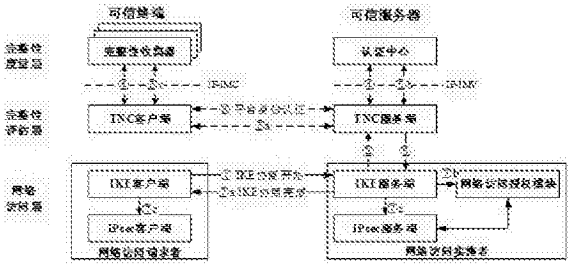
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于IPsec的可信网络连接方法

(57)摘要

本发明属于可信网络连接(TNC)技术领域，具体而言，本发明涉及一种基于IPsec的可信网络连接方法，使得终端和服务器之间通过IKE会话，周期性更新安全联盟(SA)时，也周期性进行了双向平台身份认证、完整性验证。从而既保证了终端平台的动态可信，保证了应用服务器的访问安全；也保证了终端从网络中获取的服务可信。



CN 104079570 B

1.一种基于IPsec的可信网络连接方法，基于一个基本架构，即：可信终端在访问可信服务器的过程中，底层通讯通路使用IPsec安全通道，IPsec安全通道所使用安全联盟的生命周期结束前，需要双方进行IKE会话，生成新的安全联盟；其特征在于，包括以下步骤：

步骤1、IKE客户端向IKE服务端发起密钥协商；成功后IKE服务端通知TNC服务端有一个IKE协商请求到来，若不成功则整个步骤结束；

步骤2、TNC服务端和TNC客户端进行双向平台验证，并根据验证结果进行如下操作：

选择操作一：TNC客户端和TNC服务端之间的平台验证成功完成，TNC服务端通知认证中心新的IKE协商请求已经发生，需要进行完整性验证；同时TNC客户端通知完整性收集器新的IKE协商请求已经发生，需要准备完整性相关信息；完整性收集器向TNC客户端返回平台完整性消息；并继续进行下一步的操作；

选择操作二：TNC客户端和TNC服务端之间的平台验证失败，则整个步骤结束；

步骤3、完整性收集器和认证中心之间进行完整性消息交换、验证，该完整性消息交换、验证通过TNC客户端和TNC服务端进行；同时完整性消息将会被IPsec客户端、IPsec服务端转发，直到可信终端的完整性状态满足TNC服务端的要求；

所述的完整性消息交换、验证的具体方法是：

步骤3.1、TNC客户端和TNC服务端交换完整性验证相关的各种信息；这些信息将会被IPsec客户端、IPsec服务端转发，直到可信终端的完整性状态满足TNC服务端的要求；

步骤3.2、TNC服务端将每个完整性收集器收集的完整性信息发送给认证中心；认证中心对完整性收集器收集的完整性信息进行分析，如果认证中心需要更多的完整性信息，它将通过IF-IMV接口向TNC服务端发送信息；如果认证中心已经对完整性收集器收集的完整性信息做出判断，它将结果通过IF-IMV接口发送给TNC服务端；

步骤3.3、TNC客户端也要转发来自TNC服务端的信息给相应的完整性收集器，并将来自完整性收集器的信息发给TNC服务端；

步骤4、当TNC服务端完成和TNC客户端的完整性验证握手之后，它发送TNC服务端推荐操作给IKE服务端；

步骤5、IKE服务端将IKE协商的结果通知相关各方；

具体需要通知的对象如下：

通知对象一：IKE服务端将IKE协商结果通知给IKE客户端，IKE协商完成；

通知对象二：IKE服务端将IKE协商结果通知给网络访问授权模块，并根据协商结果对该终端的访问控制策略进行更新；具体是：若IKE协商结果为协商成功，则对网络访问授权模块的访问控制策略进行禁止访问的更新；若IKE协商结果为协商失败，则对网络访问授权模块的访问控制策略进行允许访问的更新；

通知对象三：IKE服务端将协商成功的终端与服务器之间安全联盟通告给IPsec服务端，IKE客户端将协商成功的终端与服务器之间安全联盟通告给IPsec客户端。

一种基于IPsec的可信网络连接方法

技术领域

[0001] 本发明属于可信网络连接(TNC)技术领域，具体而言，本发明涉及一种基于IPsec的可信网络连接方法。

背景技术

[0002] 在标准的可信网络连接(TNC)架构中，只是在终端接入网络的过程中对终端进行了平台身份认证与完整性验证，在终端接入网络之后就没有相应的措施对网络和终端进行保护。终端平台有可能在接入后发生可信状态的改变，因此有必要增加整个接入过程的控制机制，保证终端平台的动态可信。

[0003] 同时，传统可信网络连接(TNC)的出发点是保证网络的安全性，因此该架构没有考虑如何保护终端的安全。终端在接入网络之前，除了要提供自身的平台可信性证据之外，还应该具有对接入网络进行可信性评估，否则无法保证从网络中获取的服务可信。

发明内容

[0004] 本发明主要是解决现有技术所存在的技术问题，提供一种能够使终端和服务器之间通过IKE会话，周期性更新安全联盟(SA)时，也周期性进行了双向平台身份认证、完整性验证，从而既保证了终端平台的动态可信、应用服务器的访问安全，也保证了终端从网络中获取的服务可信的一种基于IPsec的可信网络连接方法

[0005] 本发明的上述技术问题主要是通过下述技术方案得以解决的：

[0006] 一种基于IPsec的可信网络连接方法，基于一个基本架构，即：可信终端在访问可信服务器的过程中，底层通讯通路使用IPsec安全通道，IPsec安全通道所使用安全联盟的生命周期结束前，需要双方进行IKE会话，生成新的安全联盟；其特征在于，包括以下步骤：

[0007] 步骤1、IKE客户端向IKE服务端发起密钥协商；成功后IKE服务端通知TNC服务端有一个IKE协商请求到来，若不成功则整个步骤结束；

[0008] 步骤2、TNC服务端和TNC客户端进行双向平台验证，并根据验证结果进行如下操作：

[0009] 选择操作一：TNC客户端和TNC服务端之间的平台验证成功完成，TNC服务端通知认证中心新的IKE协商请求已经发生，需要进行完整性验证。同时TNC客户端通知完整性收集器新的IKE协商请求已经发生，需要准备完整性相关信息。完整性收集器向TNC客户端返回平台完整性消息；并继续进行下一步的操作；

[0010] 选择操作二：TNC客户端和TNC服务端之间的平台验证失败，则整个步骤结束；

[0011] 步骤3、完整性收集器和认证中心之间进行完整性消息交换、验证，该完整性消息交换、验证通过TNC客户端和TNC服务端进行；同时完整性消息将会被IPsec客户端、IPsec服务端转发，直到可信终端的完整性状态满足TNC服务端的要求；

[0012] 步骤4、当TNC服务端完成和TNC客户端的完整性验证握手之后，它发送TNC服务端推荐操作给IKE服务端；

[0013] 步骤5、IKE服务端将IKE协商的结果通知相关各方。

[0014] 在上述的一种基于IPsec的可信网络连接方法，所述步骤3中，完整性消息交换、验证的具体方法是：

[0015] 步骤3.1、TNC客户端和TNC服务端交换完整性验证相关的各种信息。这些信息将会被IPsec客户端、IPsec服务端转发，直到可信终端的完整性状态满足TNC服务端的要求。

[0016] 步骤3.2、TNC服务端将每个完整性收集器收集的完整性信息发送给认证中心。认证中心对完整性收集器收集的完整性信息进行分析，如果认证中心需要更多的完整性信息，它将通过IF-IMV接口向TNC服务端发送信息。如果认证中心已经对完整性收集器收集的完整性信息做出判断，它将结果通过IF-IMV接口发送给TNC服务端。

[0017] 步骤3.3、TNC客户端也要转发来自TNC服务端的信息给相应的完整性收集器，并将来自完整性收集器的信息发给TNC服务端。

[0018] 在上述的一种基于IPsec的可信网络连接方法，所述步骤5中，具体需要通知的对象如下：

[0019] 通知对象一：IKE服务端将IKE协商结果通知给IKE客户端，IKE协商完成；

[0020] 通知对象二：IKE服务端将IKE协商结果通知给网络访问授权模块，并根据协商结果对该终端的访问控制策略进行更新；具体是：若IKE协商结果为协商成功，则对网络访问授权模块的访问控制策略进行禁止访问的更新；若IKE协商结果为协商失败，则对网络访问授权模块的访问控制策略进行允许访问的更新；

[0021] 通知对象三：IKE服务端将协商成功的终端与服务器之间安全联盟通告给IPsec服务端，IKE客户端将协商成功的终端与服务器之间安全联盟通告给IPsec客户端。

[0022] 因此，本发明具有如下优点：能够使终端和服务器之间通过IKE会话，周期性更新安全联盟(SA)时，也周期性进行了双向平台身份认证、完整性验证。从而既保证了终端平台的动态可信、应用服务器的访问安全；也保证了终端从网络中获取的服务可信。

附图说明

[0023] 附图1是本发明的一种方法原理示意图。

具体实施方式

[0024] 下面通过实施例并结合附图对本发明的技术方案作进一步具体的说明。

[0025] 实施例：

[0026] 可信终端在访问可信服务器的过程中，底层通讯通路使用的是IPsec安全通道。IPsec安全通道所使用安全联盟(SA)的生命周期结束前，需要双方进行IKE会话，生成新的安全联盟(SA)。

[0027] 本专利将平台身份认证、完整性验证加入IKE会话连接建立的过程中，使得终端和服务器之间通过IKE会话，周期性更新安全联盟(SA)时，也周期性进行了平台身份认证、完整性验证。步骤如下：

[0028] 1) IKE客户端向IKE服务端发起协商，第一步进行密钥协商。

[0029] 2) IKE客户端和IKE服务端之间密钥协商成功，则IKE服务端通知TNC服务端有一个IKE协商请求到来。

[0030] 3)TNC服务端和TNC客户端进行双向平台验证。

[0031] 4)假定TNC客户端和TNC服务端之间的平台验证成功完成,TNC服务端通知认证中心新的IKE协商请求已经发生,需要进行完整性验证。同时TNC客户端通知完整性收集器新的IKE协商请求已经发生,需要准备完整性相关信息。完整性收集器向TNC客户端返回平台完整性消息。

[0032] 5)第五步主要涉及完整性收集器、认证中心之间进行完整性消息交换、验证

[0033] a)TNC客户端和TNC服务端交换完整性验证相关的各种信息。这些信息将会被IPsec客户端、IPsec服务端转发,直到可信终端的完整性状态满足TNC服务端的要求。

[0034] b)TNC服务端将每个完整性收集器收集的完整性信息发送给认证中心。认证中心对完整性收集器收集的完整性信息进行分析,如果认证中心需要更多的完整性信息,它将通过IF-IMV接口向TNC服务端发送信息。如果认证中心已经对完整性收集器收集的完整性信息做出判断,它将结果通过IF-IMV接口发送给TNC服务端。

[0035] c) TNC客户端也要转发来自TNC服务端的信息给相应的完整性收集器,并将来自完整性收集器的信息发给TNC服务端。

[0036] 6) 当TNC服务端完成和TNC客户端的完整性验证握手之后,它发送TNC服务端推荐操作给IKE服务端;

[0037] 7) IKE服务端将IKE协商的结果通知相关各方,

[0038] a) IKE服务端将IKE协商结果通知给IKE客户端,IKE协商完成;

[0039] b) IKE服务端将IKE协商结果通知给网络访问授权模块,并根据协商结果(成功OR失败)对该终端的访问控制策略进行更新(禁止访问OR允许访问);

[0040] c)IKE服务端将协商成功的终端与服务器之间安全联盟(SA)通告给IPsec服务端,IKE客户端将协商成功的终端与服务器之间安全联盟(SA)通告给IPsec客户端。

[0041] 到此,一次完整的IKE会话结束。在IKE会话中,服务器再次确认终端的平台身份、完整性状态后,终端和服务器使用新的安全联盟(SA)建立IPsec通道,传输终端访问应用服务器的数据包。

[0042] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代,但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。

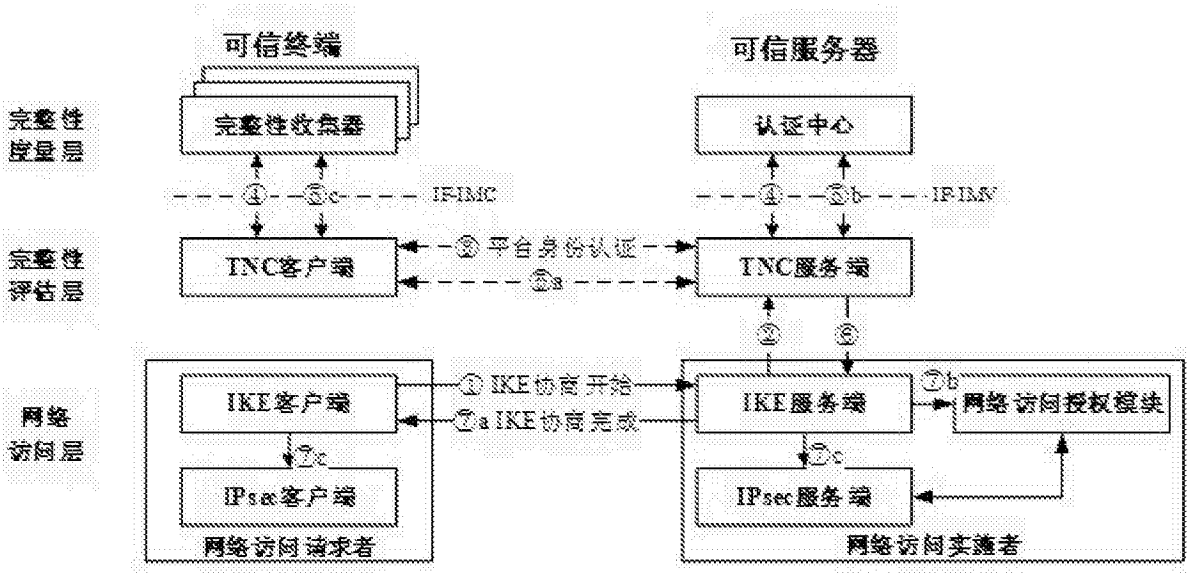

可信终端
可信服务器
完整性度量层
完整性评估层
网络访问层
完整性收集器
认证中心
IF-IMC
IF-IMV
TNC客户端
TNC服务端
平台身份认证
IKE客户端
IKE服务端
网络访问授权模块
IKE协商开始
IKE协商完成
IPsec客户端
IPsec服务端
网络访问请求者
网络访问实施者

图1