(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105407092 A
(43)申请公布日 2016.03.16

(21)申请号 201510737480.4

(22)申请日 2015.11.04

(71)申请人 北京汉柏科技有限公司
地址 100085 北京市海淀区上地十街1号院5号楼5层511室

(72)发明人 陈海滨

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

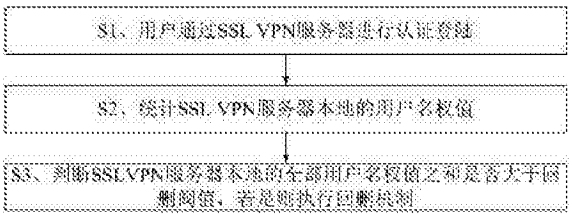
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种VPN用户认证方法及装置

(57)摘要

本发明提供一种VPN用户认证方法及装置，其中，所述方法包括：S1、用户通过SSL VPN服务器进行认证登陆；S2、统计SSL VPN服务器本地的用户名权值；S3、判断SSL VPN服务器本地的全部用户名权值之和是否大于回删阀值，若是则执行回删机制。上述方法有效的提高用户的体验效果，节约了升级硬件的成本。



CN 105407092 A

1.一种 VPN 用户认证方法，其特征在于，所述方法包括：

S1、用户通过 SSL VPN 服务器进行认证登陆；

S2、统计 SSL VPN 服务器本地的用户名权值；

S3、判断 SSL VPN 服务器本地的全部用户名权值之和是否大于回删阀值，若是，则执行回删机制。

2.根据权利要求 1 所述的方法，其特征在于，所述用户通过 SSL VPN 服务器进行认证登陆，还包括：

S11、用户通过用户名和密码访问 SSL VPN 服务器进行认证登陆，SSL VPN 服务器将所述用户名和密码与 SSL VPN 服务器本地存储的用户名和密码进行比对，若 SSL VPN 服务器本地没有所述用户名和密码，则执行步骤 S12；若 SSL VPN 服务器本地有所述用户名和密码，则执行步骤 S13；

S12、将所述用户名和密码发往认证服务器进行用户认证，并将所述用户名和密码记录到 SSL VPN 服务器本地的临时用户表中，之后执行步骤 S14；

S13、判断所述用户名和密码的状态，若所述用户名和密码标记为可用，则返回给用户相应的结果；若所述用户名和密码正在等待认证服务器获取结果中，则执行步骤 S14；

S14、SSL VPN 服务器接收到认证服务器返回的认证结果后，判断所述认证结果，若认证失败，则删除 SSL VPN 服务器本地的临时用户表中的所述用户名和密码，若认证成功，则将所述用户名和密码记录到 SSL VPN 服务器本地的用户列表中，并返回给用户相应的结果。

3.根据权利要求 1 所述的方法，其特征在于，所述统计 SSL VPN 服务器本地的用户名权值，具体为：

当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN 服务器将所述用户使用的用户名的权值设置为 2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加 1；当用户下线时，将所述用户使用的用户名的权值减 1；当用户连续在线每超过 24 小时时，将所述用户使用的用户名的权值加 1。

4.根据权利要求 1 所述的方法，其特征在于，所述回删机制，具体为：

判断是否存在权值是 1 的用户名，若是，则将权值是 1 的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减 1 后，并将当前权值最小的用户名对应的用户名和密码删除。

5.一种 VPN 用户认证装置，其特征在于，所述装置包括：

认证单元，负责用户通过 SSL VPN 服务器进行认证登陆；

统计单元，用于统计 SSL VPN 服务器本地的用户名权值；

判断单元，用于判断 SSL VPN 服务器本地的全部用户名权值之和是否大于回删阀值，若是则执行回删机制。

6.根据权利要求 5 所述装置，其特征在于，所述统计单元，用于统计 SSL VPN 服务器本地的用户名权值，具体为：

当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN 服务器将所述用户使用的用户名的权值设置为 2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加 1；当用户下线时，将所述用户使用的用户名的权值减 1；当用户连续在线每超过 24 小时时，将所述用户使用的用户名的权值加 1。

7. 根据权利要求 5 所述装置，其特征在于，所述判断单元还包括：

回删子单元，用于判断是否存在权值是 1 的用户名，若是，则将权值是 1 的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减 1 后，并将当前权值最小的用户名对应的用户名和密码删除。

一种 VPN 用户认证方法及装置

技术领域

[0001] 本发明涉及网络通信技术领域，尤其涉及一种 VPN 用户认证方法及装置。

背景技术

[0002] SSL VPN 功能专门用于在用户进行大规模认证后的权限控制，其中用户认证是关键的环节，涉及到用户认证超时和等待认证结果的效率问题，在当前 SSL VPN 功能中，通常使用的方法是，一个账号可以被多个用户进行认证使用，其中，不同的用户携带同一个账号进行认证时，每个用户都需要 SSL VPN 设备与认证设备进行一次交互认证过程，此过程由于不是在一个设备上完成，导致 SSL VPN 设备与认证设备之前进行多次认证消息交互，每个用户等待的时间都会很长，这样就造成了用户体验差的情况，更有多用户同时并发认证，导致认证服务器繁忙导致认证消息丢失从而认证失败的情况经常发生。

[0003] 目前，主要通过提高设备性能和利用多台 SSL VPN 设备与认证设备，扁平化分担用户的并发处理能力，但是这样也势必造成设备成本增加。

发明内容

[0004] 为了能够在同样的设备条件下提高用户的体验效果，本发明提出了一种 VPN 用户认证方法及装置，具体方案如下：

一种 VPN 用户认证方法，其特征在于，所述方法包括：

S1、用户通过 SSL VPN 服务器进行认证登陆；

S2、统计 SSL VPN 服务器本地的用户名权值；

S3、判断 SSL VPN 服务器本地的全部用户名权值之和是否大于回删阀值，若是，则执行回删机制。

[0005] 优选的，所述用户通过 SSL VPN 服务器进行认证登陆，还包括：

S11、用户通过用户名和密码访问 SSL VPN 服务器进行认证登陆，SSL VPN 服务器将所述用户名和密码与 SSL VPN 服务器本地存储的用户名和密码进行比对，若 SSL VPN 服务器本地没有所述用户名和密码，则执行步骤 S12；若 SSL VPN 服务器本地有所述用户名和密码，则执行步骤 S13；

S12、将所述用户名和密码发往认证服务器进行用户认证，并将所述用户名和密码记录到 SSL VPN 服务器本地的临时用户表中，之后执行步骤 S14；

S13、判断所述用户名和密码的状态，若所述用户名和密码标记为可用，则返回给用户相应的结果；若所述用户名和密码正在等待认证服务器获取结果中，则执行步骤 S14；

S14、SSL VPN 服务器接收到认证服务器返回的认证结果后，判断所述认证结果，若认证失败，则删除 SSL VPN 服务器本地的临时用户表中的所述用户名和密码，若认证成功，则将所述用户名和密码记录到 SSL VPN 服务器本地的用户列表中，并返回给用户相应的结果。

[0006] 优选的，所述统计 SSL VPN 服务器本地的用户名权值，具体为：

当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN 服务器将所述

用户使用的用户名的权值设置为 2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加 1；当用户下线时，将所述用户使用的用户名的权值减 1；当用户连续在线每超过 24 小时时，将所述用户使用的用户名的权值加 1。

[0007] 优选的，所述回删机制，具体为：

判断是否存在权值是 1 的用户名，若是，则将权值是 1 的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减 1 后，并将当前权值最小的用户名对应的用户名和密码删除。

[0008] 优选的，所述装置包括：

认证单元，负责用户通过 SSL VPN 服务器进行认证登陆；

统计单元，用于统计 SSL VPN 服务器本地的用户名权值；

判断单元，用于判断 SSL VPN 服务器本地的全部用户名权值之和是否大于回删阀值，若是则执行回删机制。

[0009] 优选的，所述统计单元，用于统计 SSL VPN 服务器本地的用户名权值，具体为：

当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN 服务器将所述用户使用的用户名的权值设置为 2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加 1；当用户下线时，将所述用户使用的用户名的权值减 1；当用户连续在线每超过 24 小时时，将所述用户使用的用户名的权值加 1。

[0010] 优选的，所述判断单元还包括：

回删子单元，用于判断是否存在权值是 1 的用户名，若是，则将权值是 1 的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减 1 后，并将当前权值最小的用户名对应的用户名和密码删除。

[0011] 本发明提供一套解决方案，通过第一个用户使用用户名密码后，将用户名密码记录在本地，当本地用户名密码记录过多时，采用用户数据在线人数、单位时间内上线次数、上线时间等方式进行权值比较，自动分析用户的上线频率，将上线频率低，可能出现僵尸上线用户首先下线的方式，保证新近上线用户的用户名密码信息可以及时保存在本地的方法，来实现用户 SSLVPN 上线的超快体验。

附图说明

[0012] 图 1 为本发明提供的一种 VPN 用户认证方法的流程示意图；

图 2 为本发明提供的一种 VPN 用户认证装置的结构示意图。

具体实施方式

[0013] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整的描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他的实施例，都属于本发明保护的范围。

[0014] 图 1 示出了本发明的一种 VPN 用户认证方法的流程示意图，具体方法如下所述：

S1、用户通过 SSL VPN 服务器进行认证登陆。

[0015] 具体的，还包含：

S11、用户通过用户名和密码访问SSL VPN服务器进行认证登陆，SSL VPN服务器将所述用户名和密码与SSL VPN服务器本地存储的用户名和密码进行比对，若SSL VPN服务器本地没有所述用户名和密码，则执行步骤S12；若SSL VPN服务器本地有所述用户名和密码，则执行步骤S13。

[0016] S12、将所述用户名和密码发往认证服务器进行用户认证，并将所述用户名和密码记录到SSL VPN服务器本地的临时用户表中，之后执行步骤S14。

[0017] S13、判断所述用户名和密码的状态，若所述用户名和密码标记为可用，则返回给用户相应的结果；若所述用户名和密码正在等待认证服务器获取结果中，则执行步骤S14。

[0018] S14、SSL VPN服务器接收到认证服务器返回的认证结果后，判断所述认证结果，若认证失败，则删除SSL VPN服务器本地的临时用户表中的所述用户名和密码，若认证成功，则将所述用户名和密码记录到SSL VPN服务器本地的用户列表中，并返回给用户相应的结果。

[0019] S2、统计SSL VPN服务器本地的用户名权值。

[0020] 具体为，当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN服务器将所述用户使用的用户名的权值设置为2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加1；当用户下线时，将所述用户使用的用户名的权值减1；当用户连续在线每超过24小时时，将所述用户使用的用户名的权值加1。

[0021] 举例说明，当用户A成功登陆时，且其使用的用户名α是首次成功登陆，那么用户名α当前的权值是2,；由于存在多用户同时登陆的情况，当用户B成功登陆时，其使用的同样是用户名α，此时用户A和用户B同时在线，那么用户名α当前的权值是3；若用户A的连续在线时间是50小时，用户B的续在线时间是36小时，那么用户名α当前的权值是6；若用户A在此之后下线，用户B继续在线，那么用户名α当前的权值是5。

[0022] S3、判断SSL VPN服务器本地的全部用户名权值之和是否大于回删阀值，若是，则执行回删机制。

[0023] 其中，所述回删机制具体为，判断是否存在权值是1的用户名，若是，则将权值是1的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减1后，并将当前权值最小的用户名对应的用户名和密码删除。

[0024] 图2示出了本发明提供的一种VPN用户认证装置的结构示意图，包括：认证单元、统计单元、判断单元和执行单元。

[0025] 认证单元，负责用户通过SSL VPN服务器进行认证登陆。

[0026] 统计单元，用于统计SSL VPN服务器本地的用户名权值。

[0027] 具体为，当用户成功登陆，且所述用户使用的用户名是首次成功登陆时，SSL VPN服务器将所述用户使用的用户名的权值设置为2；当用户使用的用户名是非首次成功登陆时，将所述用户使用的用户名的权值加1；当用户下线时，将所述用户使用的用户名的权值减1；当用户连续在线每超过24小时时，将所述用户使用的用户名的权值加1。

[0028] 判断单元，用于判断SSL VPN服务器本地的全部用户名权值之和是否大于回删阀值，若是，则执行回删机制。

[0029] 判断单元还包括，回删子单元，用于判断是否存在权值是1的用户名，若是，则将权值是1的用户名对应的用户名和密码删除；若否，则将当前没有上线的用户名的权值减1

后，并将当前权值最小的用户名对应的用户名和密码删除。

[0030] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明权利要求所限定的范围。

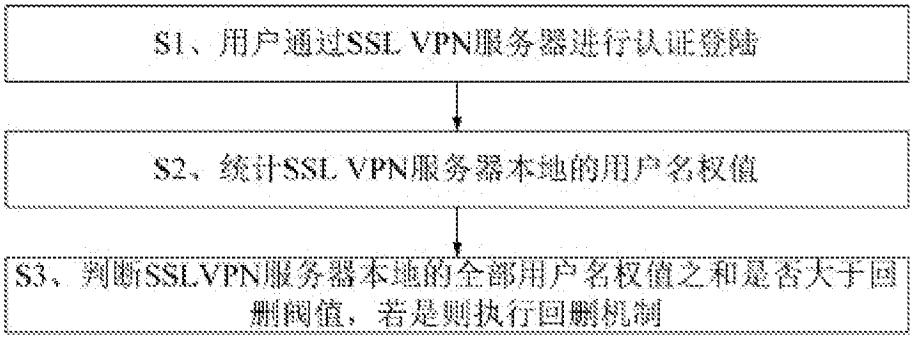

S1、用户通过SSL VPN服务器进行认证登陆
S2、统计SSL VPN服务器本地的用户名权值
S3、判断SSLVPN服务器本地的全部用户名权值之和是否大于回删阀值，若是则执行回删机制

图 1

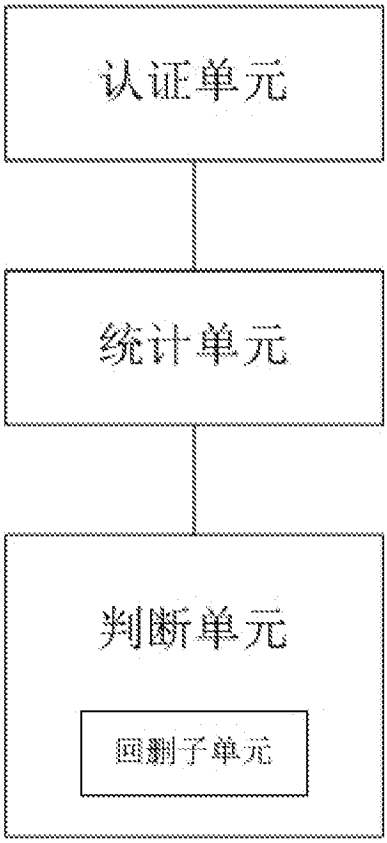

认证单元
统计单元
判断单元
回删子单元

图 2