(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112910847 B
(45)授权公告日 2023.04.07

(21)申请号 202110056573.6

(22)申请日 2021.01.15

(65)同一申请的已公布的文献号
申请公布号 CN 112910847 A

(43)申请公布日 2021.06.04

(73)专利权人 北京开物数智科技有限公司
地址 100070 北京市丰台区汽车博物馆西路8号院华夏幸福创新中心C405

(72)发明人 郭耕良

(74)专利代理机构 北京劲创知识产权代理事务所(普通合伙) 11589
专利代理师 田亚飞

(51)Int.Cl.
H04L 41/122(2022.01)
H04L 12/46(2006.01)

(56)对比文件
WO 2019207251 A1,2019.10.31
CN 107925651 A,2018.04.17
US 2020076735 A1,2020.03.05
CN 109921944 A,2019.06.21

审查员 杨柳

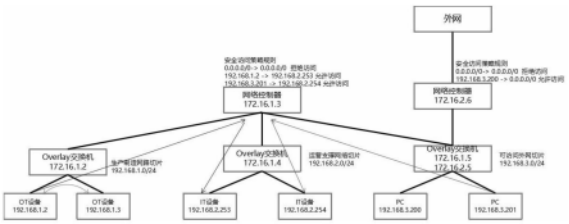
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于切片的工业网络安全实现方法

(57)摘要

本发明公开一种基于切片的工业网络安全实现方法,包括IT网络与OT网络互通,对于OT网络于IT网络使用不同协议情况,使用网关进行协议的转换;利用Overlay技术对工厂的网络进行虚拟化;基于虚拟化的网络,将网络分为生产制造网络,本发明通过IT网络与OT网络互通、利用Overlay技术对工厂的网络进行虚拟化、基于虚拟化的网络,将网络分为生产制造网络,运营支撑网络,可访问外网网络三个切片、网络切片最终终止于工厂网络控制器,三个切片间的网络访问全部经由网络控制器进行控制,不同切片中的成员默认不可以互访,需要互访的成员,只需要在网络控制器增加对应的安全访问策略即可互访通过使能将工厂网络的切片技术,工厂内不同网络可以安全互访。



CN 112910847 B

1.一种基于切片的工业网络安全实现方法,其特征在于:包括IT网络与OT网络互通,对于OT网络与IT网络使用不同协议情况,使用网关进行协议的转换;利用Overlay技术对工厂的网络进行虚拟化;基于虚拟化的网络,将网络分为生产制造网络,运营支撑网络,可访问外网网络三个切片;网络切片最终终止于工厂网络控制器,三个切片间的网络访问全部经由工厂网络控制器进行控制;工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制,工厂网络控制器能够调整三个切片的成员,使不同的成员能够灵活加入切片;

所述IT网络与OT网络互通,对于OT网络与IT网络使用不同协议情况,使用网关进行协议的转换,IT网络为不封装的IPv4/IPv6网络,这样的网络能够实现相互之间IP互通;

所述利用Overlay技术对工厂的网络进行虚拟化,工厂的网络设备使用支持Overlay技术的设备,包括实现VXLAN、MPLSoGRE、MPLSoUDP的交换机及路由器,每个交换机通过集中配置或单独配置的方式实现多个设备之间形成逻辑隧道,接入网络的设备之间通信都基于逻辑隧道,由于Overlay的封装,不在同一虚拟化网络内的设备默认无法通信,从而形成隔离的虚拟化网络,不同的设备接入交换机之后,逻辑划分到不同的虚拟化网络中。

2.根据权利要求1所述的一种基于切片的工业网络安全实现方法,其特征在于:所述基于虚拟化的网络,将网络分为生产制造网络,运营支撑网络,可访问外网网络三个切片,基于上述中的Overlay配置,划分出三个互相隔离的生产制造网络,运营支撑网络和访问外网网络,三个虚拟化网络默认相互不可通信,每个设备根据实际的需求选择逻辑接入对应的网络,逻辑接入指的是通过配置的方式将IT设备/OT设备的MAC/IP加入对应的虚拟化网络中。

3.根据权利要求1所述的一种基于切片的工业网络安全实现方法,其特征在于:所述网络切片最终终止于工厂网络控制器,三个切片间的网络访问全部经由工厂网络控制器进行控制,同一网络切片内设备的网络通信不经过工厂网络控制器,设备直接经过上述中的逻辑隧道直接通信,不同切片间的网络互访,设备的报文首先经过交换机和工厂网络控制器之间的隧道到达工厂网络控制器,经过检查后到达目的地交换机及目的设备。

4.根据权利要求1所述的一种基于切片的工业网络安全实现方法,其特征在于:所述工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制,工厂网络控制器的转发流程中提供ACL方式的安全访问策略,ACL策略根据工厂的实际需求配置。

5.根据权利要求1所述的一种基于切片的工业网络安全实现方法,其特征在于:所述工厂网络控制器能够调整三个切片的成员,使不同的成员能够灵活加入切片,不同切片中的成员默认不可以互访,需要互访的成员,只需要在工厂网络控制器增加对应的安全访问策略即可互访,已经实现的互访成员,如果不需要互访只需要删除对应的安全访问策略即可。

一种基于切片的工业网络安全实现方法

技术领域

[0001] 本发明属于工业网络安全相关技术领域，具体涉及一种基于切片的工业网络安全实现方法。

背景技术

[0002] 工业网络包括工厂的IT网络和工厂的OT网络两部分。IT网络负责工厂信息化部分，如ERP系统，MES系统等，工厂的OT网络负责工厂的生产制造，如智能化机床，各种传感器，信息采集系统等。通常情况下，IT网络为OT网络制定生产计划，下发生产任务等；OT网络为IT网络提供生成数据，因此这两个网络需要互联互通。

[0003] 现有的技术存在以下问题：IT网络的不安全性，一旦IT网络被攻击就会严重影响OT网络，最终对工厂的生产造成影响，因此很多工厂没有将IT网络和OT网络互通，对生产效率产生一定的影响。

发明内容

[0004] 本发明的目的在于提供一种基于切片的工业网络安全实现方法，以解决上述背景技术中提出的IT网络的不安全性，一旦IT网络被攻击就会严重影响OT网络，最终对工厂的生产造成影响，因此很多工厂没有将IT网络和OT网络互通，对生产效率产生一定的影响的问题。

[0005] 为实现上述目的，本发明提供如下技术方案：

[0006] 一种基于切片的工业网络安全实现方法，包括IT网络与OT网络互通，对于OT网络于IT网络使用不同协议情况，使用网关进行协议的转换；利用Overlay技术对工厂的网络进行虚拟化；基于虚拟化的网络，将网络分为生产制造网络，运营支撑网络，可访问外网网络三个切片；网络切片最终终止于工厂网络控制器，三个切片间的网络访问全部经由网络控制器进行控制；工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制和工厂网络控制器可以调整三个切片的成员，使不同的成员可以灵活加入切片。

[0007] 优选的，所述IT网络与OT网络互通，对于OT网络于IT网络使用不同协议情况，使用网关进行协议的转换，IT网络一般情况为不封装的IPv4/IPv6网络，这样的网络可以实现相互之间IP互通。

[0008] 优选的，所述利用Overlay技术对工厂的网络进行虚拟化，工厂的网络设备使用支持Overlay技术的设备，主要是指实现VXLAN、MPLSoGRE、MPLSoUDP的交换机及路由器，每个交换机通过配置的方式(集中配置或单独配置)，实现多个设备之间形成N*(N-1)的逻辑隧道，接入网络的设备之间通信都基于逻辑隧道，由于Overlay的封装，不在同一虚拟化网络内的设备默认无法通信，从而形成隔离的虚拟化网络，不同的设备接入交换机之后，逻辑划分到不同的虚拟化网络中。

[0009] 优选的，所述基于虚拟化的网络，将网络分为生产制造网络，运营支撑网络，可访问外网网络三个切片，基于上述中的Overlay配置，划分出三个互相隔离的生产制造网络，

运营支撑网络和访问外网网络,三个虚拟化网络默认相互不可通信,每个设备根据实际的需求选择逻辑接入对应的网络,逻辑接入指的是通过配置的方式将IT设备/OT设备的MAC/IP加入对应的虚拟化网络中。

[0010] 优选的,所述网络切片最终终止于工厂网络控制器,三个切片间的网络访问全部经由网络控制器进行控制,同一网络切片内设备的网络通信不经过工厂网络控制器,设备直接经过上述中的逻辑隧道直接通信,不同切片间的网络互访,设备的报文首先经过交换机和网络控制器之间的隧道到达网络控制器,经过检查后再由未来之器到达目的地交换机及目的设备。

[0011] 优选的,所述工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制,网络控制器的转发流程中提供ACL方式的安全访问策略,ACL策略根据工厂的实际需求配置。

[0012] 优选的,所述工厂网络控制器可以调整三个切片的成员,使不同的成员可以灵活加入切片,不同切片中的成员默认不可以互访,需要互访的成员,只需要在网络控制器增加对应的安全访问策略即可互访,已经实现的互访成员,如果不需要互访只需要删除对应的安全访问策略即可。

[0013] 与现有技术相比,本发明提供了一种基于切片的工业网络安全实现方法,具备以下有益效果:

[0014] 本发明通过IT网络与OT网络互通、利用Overlay技术对工厂的网络进行虚拟化、基于虚拟化的网络,将网络分为生产制造网络,运营支撑网络,可访问外网网络三个切片、网络切片最终终止于工厂网络控制器,三个切片间的网络访问全部经由网络控制器进行控制,工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制,工厂网络控制器可以调整三个切片的成员,使不同的成员可以灵活加入切片,不同切片中的成员默认不可以互访,需要互访的成员,只需要在网络控制器增加对应的安全访问策略即可互访,已经实现的互访成员,如果不需要互访只需要删除对应的安全访问策略即可,通过使能将工厂网络的切片技术,工厂内不同网络可以安全互访。

附图说明

[0015] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例一起用于解释本发明,并不构成对本发明的限制,在附图中:

[0016] 图1为本发明提出的一种基于切片的工业网络安全实现方法结构示意图;

[0017] 图中:1、OT设备、IT设备、PC的接入交换机均为支持Overlay技术的交换机;

[0018] 2、Overlay交换及网络控制器之间网络可达(IP可达,可以是IPv4或IPv6,图中以IPv4示意);

[0019] 3、Overlay交换机及网络控制器之间根据实际需要部署一个或者多个,图中分为内网的网络控制器及外网的网络控制器;

[0020] 4、三个切片网络分别为不同的用途,接入的设备分配的地址为切片网络地址;

[0021] 5、网络控制器中默认不允许跨切片的访问,增加对应的安全策略后,跨切片的特定设备之间可以相互访问;

[0022] 6、同一切片内的设备互访不需要经过网络控制器。

具体实施方式

[0023] 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、完整地描述，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。基于本发明中的实施例，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实施例，都属于本发明保护的范围。

[0024] 请参阅图1，本发明提供一种技术方案：

[0025] 一种基于切片的工业网络安全实现方法，包括IT网络与OT网络互通，对于OT网络于IT网络使用不同协议情况，使用网关进行协议的转换；利用Overlay技术对工厂的网络进行虚拟化；基于虚拟化的网络，将网络分为生产制造网络，运营支撑网络，可访问外网网络三个切片；网络切片最终终止于工厂网络控制器，三个切片间的网络访问全部经由网络控制器进行控制；工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制和工厂网络控制器可以调整三个切片的成员，使不同的成员可以灵活加入切片。

[0026] IT网络与OT网络互通，对于OT网络于IT网络使用不同协议情况，使用网关进行协议的转换，IT网络一般情况为不封装的IPv4/IPv6网络，这样的网络可以实现相互之间IP互通；利用Overlay技术对工厂的网络进行虚拟化，工厂的网络设备使用支持Overlay技术的设备，主要是指实现VXLAN、MPLSoGRE、MPLSoUDP的交换机及路由器，每个交换机通过配置的方式(集中配置或单独配置)，实现多个设备之间形成N*(N-1)的逻辑隧道，接入网络的设备之间通信都基于逻辑隧道，由于Overlay的封装，不在同一虚拟化网络内的设备默认无法通信，从而形成隔离的虚拟化网络，不同的设备接入交换机之后，逻辑划分到不同的虚拟化网络中；基于虚拟化的网络，将网络分为生产制造网络，运营支撑网络，可访问外网网络三个切片，基于上述中的Overlay配置，划分出三个互相隔离的生产制造网络，运营支撑网络和访问外网网络，三个虚拟化网络默认相互不可通信，每个设备根据实际的需求选择逻辑接入对应的网络，逻辑接入指的是通过配置的方式将IT设备/OT设备的MAC/IP加入对应的虚拟化网络中；网络切片最终终止于工厂网络控制器，三个切片间的网络访问全部经由网络控制器进行控制，同一网络切片内设备的网络通信不经过工厂网络控制器，设备直接经过上述中的逻辑隧道直接通信，不同切片间的网络互访，设备的报文首先经过交换机和网络控制器之间的隧道到达网络控制器，经过检查后再由未来之器到达目的地交换机及目的设备；工厂网络控制器集成安全访问策略对于跨切片的访问进行安全控制，网络控制器的转发流程中提供ACL方式的安全访问策略，ACL策略根据工厂的实际需求配置；工厂网络控制器可以调整三个切片的成员，使不同的成员可以灵活加入切片，不同切片中的成员默认不可以互访，需要互访的成员，只需要在网络控制器增加对应的安全访问策略即可互访，已经实现的互访成员，如果不需要互访只需要删除对应的安全访问策略即可。

[0027] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。

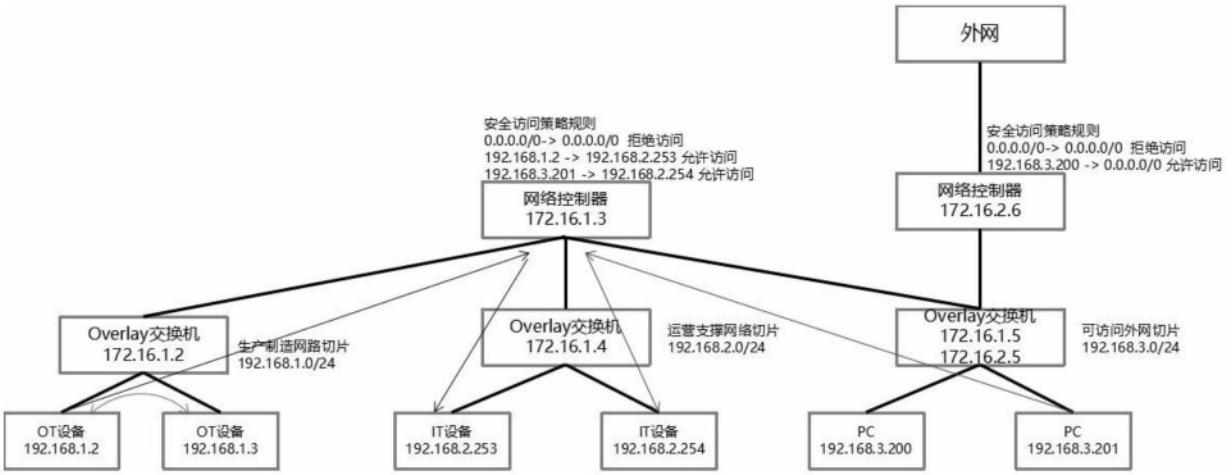

外网
安全访问策略规则
0.0.0.0/0-> 0.0.0.0/0 拒绝访问
192.168.1.2 -> 192.168.2.253 允许访问
192.168.3.201 -> 192.168.2.254 允许访问
网络控制器
172.16.1.3
安全访问策略规则
0.0.0.0/0-> 0.0.0.0/0 拒绝访问
192.168.3.200 -> 0.0.0.0/0 允许访问
网络控制器
172.16.2.6
Overlay交换机
172.16.1.2
生产制造网路切片
192.168.1.0/24
Overlay交换机
172.16.1.4
运营支撑网络切片
192.168.2.0/24
Overlay交换机
172.16.1.5
172.16.2.5
可访问外网切片
192.168.3.0/24
OT设备
192.168.1.2
OT设备
192.168.1.3
IT设备
192.168.2.253
IT设备
192.168.2.254
PC
192.168.3.200
PC
192.168.3.201

图1