国 际 电 信 联 盟

ITU-T X.1042

(01/2019)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

信息和网络安全 – 网络安全

使用软件定义网络的安全业务

ITU-T X.1042建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1 – X.199
开放系统互连	X.200 – X.299
网间互通	X.300 – X.399
报文处理系统	X.400 – X.499
号码簿	X.500 – X.599
OSI组网和系统概貌	X.600 – X.699
OSI管理	X.700 – X.799
安全	X.800 – X.849
OSI应用	X.850 – X.899
开放分布式处理	X.900 – X.999
信息和网络安全	
一般安全问题	X.1000 – X.1029
网络安全	**X.1030 – X.1049**
安全管理	X.1050 – X.1069
生物测定	X.1080 – X.1099
安全应用和服务	
组播安全	X.1100 – X.1109
家庭网络安全	X.1110 – X.1119
移动安全	X.1120 – X.1139
网页安全	X.1140 – X.1149
安全协议	X.1150 – X.1159
对等网络安全	X.1160 – X.1169
网络身份安全	X.1170 – X.1179
PITV安全	X.1180 – X.1199
网络空间安全	
计算网络安全	X.1200 – X.1229
反垃圾信息	X.1230 – X.1249
身份管理	X.1250 – X.1279
安全应用和服务	
应急通信	X.1300 – X.1309
泛在传感器网络安全	X.1310 – X.1339
PKI相关建议书	X.1340 – X.1349
网络安全信息交换	
网络安全综述	X.1500 – X.1519
脆弱性/状态信息交换	X.1520 – X.1539
事件/事故/探索法信息交换	X.1540 – X.1549
政策的交换	X.1550 – X.1559
探索法和信息要求	X.1560 – X.1569
标示和发现	X.1570 – X.1579
确保交换	X.1580 – X.1589
云计算安全	
云计算安全综述	X.1600 – X.1601
云计算安全设计	X.1602 – X.1639
云计算安全最佳实践和指导原则	X.1640 – X.1659
云计算安全实现	X.1660 – X.1679
其他云计算安全	X.1680 – X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1042建议书

使用软件定义网络的安全业务

摘要

ITU-T X.1042建议书支持对使用基于软件定义网络（SDN）安全业务的网络资源形成保护。首先，本建议书对基于SDN的安全业务网络资源进行分类：SDN应用、SDN控制器、SDN交换机和安全管理器（SM）。之后，ITU-T X.1042建议书对基于SDN的安全业务作出规定。

历史沿革

版本	建议书	批准日期	研究组	唯一ID*
1.0	ITU-T X.1042	2019-01-30	17	11.1002/1000/13803

关键词

接入控制、DDoS攻击、防火墙、蜜罐、软件定义网络（SDN）、安全情形。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1042建议书

使用软件定义网络的安全业务

1 范围

本建议书支持使用基于软件定义网络（SDN）安全业务的网络资源保护。本建议书涵盖括：

– 可由基于SDN的安全业务保护的网络资源的分类；

– 基于SDN的安全业务定义；

– 基于SDN的安全业务实施规范。

基于SDN的安全业务对网络资源（如路由器、交换机、防火墙和入侵检测系统）的保护意味着：

– 对新的网络攻击[例如蠕虫和分布式拒绝服务（DDoS）攻击做出快速反应]；

– 构建专用网络以减轻复杂的网络攻击；

– 在没有网络管理员干预的情况下自动防御网络攻击；

– 动态网络负载感知资源分配。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T Y.3300] ITU-T Y.3300建议书（2014年）– 软件定义网络的框架。

[ITU-T Y.3301] ITU-T Y.3301建议书（2016年）– 软件定义网络的功能要求。

[ITU-T Y.3302] ITU-T Y.3302建议书（2017年）– 软件定义网络的功能架构。

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 软件定义网络[ITU-T Y.3300]：能够促成对网络资源直接进行编程、编排、控制和管理的一系列技术，这些技术便于人们以灵活多变和可扩展方式设计、交付和运营网络业务。

3.1.2 接入控制[b-ITU-T X.1252]：用来确定一实体是否应按照预先确定的规则和请求方的具体权利或相关授权被授予获得资源、设施、服务或信息的程序。

3.1.3 接入控制政策[b-ITU-T X.812]：确定可进行接入的条件的一系列规则。

3.1.4 接入控制政策规则[b-ITU-T X.812]：关于接入控制业务提供的安全政策规则。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 网络资源：在网络系统中进行数据包传送的网络装置。

注 – 网络资源包括网络交换机、路由器、网关、WiFi接入点。

3.2.2 防火墙：在网络的两个组成部分连接处的一种装置或业务，对每一个企图跨越网络边界的数据包进行检查。防火墙还摒弃不符合特定标准（如已废除的端口号或IP地址）的任何数据包。

注 – 防火墙业务可以与物理设备分离，并作为应用程序工作。

3.2.3 蜜罐：为引诱网络攻击者而建立的计算机安全机制，用于检测或转移来自合法目标的攻击，并收集攻击数据。蜜罐这一术语源自其行为 – 将攻击者（“蜜蜂”）吸引至某一地方（攻击目标或“蜂蜜”），即设下陷阱。

3.2.4 集中式防火墙业务：集中式防火墙业务是为了进行有效防火墙管理而在网络资源之间建立和分布接入控制政策规则。这些规则可由集中式服务器进行动态管理。软件定义网络（SDN）可通过防火墙应用与网络资源之间的标准接口作为集中式防火墙业务工作。

3.2.5 集中式DDoS攻击减缓业务：一种业务，可以建立接入控制政策规则并将其分发到网络资源中，以有效减轻分布式拒绝服务（DDoS）攻击。这些规则可由集中式服务器以动态方式进行管理。软件定义网络（SDN）可通过DDoS攻击减缓应用与网络资源之间的标准接口作为集中式DDoS攻击减缓业务工作。

3.2.6 集中式蜜罐业务：集中式蜜罐业务在网络资源之间建立和分布接入控制政策规则，以实现动态蜜罐配置。这些规则可由集中式服务器进行动态管理。软件定义网络（SDN）可通过蜜罐应用与网络资源之间的标准接口作为集中式蜜罐业务工作。

3.2.7 集中式非法装置管理业务：集中式非法装置管理业务可以在网络资源之间建立和分布接入控制政策规则，以建立起非法装置黑名单。这些规则可由集中式服务器动态和全面地进行管理。软件定义网络（SDN）可通过非法装置管理应用与网络资源之间的标准接口作为基于网络的非法装置管理器工作。

注 – 关于非法装置的标准不属于本建议书的范围。举例而言，非法装置可以根据全球唯一识别系统的使用来确定。

3.2.8 接入控制管理业务：接入控制管理业务可以在网络资源之间建立和分布接入权利政策，以建立起物联网（IoT）装置白名单。这些政策可由集中式服务器动态和全面地进行管理。软件定义网络（SDN）可通过接入控制应用与网络资源之间的标准接口作为基于网络的IoT管理器工作。

注 – 接入政策分层组合的规范不在本建议书的范围内。这些接入政策可以根据网络资源的安全级别和在网络系统中的分布到进行组合和划分。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

ACI	应用控制接口
ACM	接入控制管理
AL-MSO	应用层管理支持和编排
ALM	应用层管理
BSS	业务支持系统
CL-AS	控制层应用支持
CL-CLS	控制层控制层业务
CL-MSO	控制层管理支持和编排
CL-RA	控制层资源抽象
CLM	控制层管理
DDoS	分布式拒绝服务
DNS	域名业务
DPI	深层数据包检查
I2NSF	至网络安全功能的接口
IoT	物联网
IP	互联网协议
MAC	媒体接入控制
MMF	多层管理功能
MMFA	多层管理功能应用层
MMFC	多层管理功能控制层
MMFO	多层管理功能OSS/BSS
MMFR	多层管理功能资源层
NSF	网络安全功能
OSS	操作支持系统
RCI	资源控制接口
RLM	资源层管理
RL-MS	资源层管理支持
SDN	软件定义网络
SDN-AL	软件定义网络 – 应用层
SDN-CL	软件定义网络 – 控制层
SDN-RL	软件定义网络 – 资源层
SIP	会话起始协议
SM	安全管理器

TCP 传输控制协议

VoIP 互联网协议语音

VoLTE 长期演进语音

5 惯例

本建议书中：

关键词“要求”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“建议”表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键词“禁止”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键词“作为选择可以”表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，厂商可以作为选择提供这一功能，同时仍然声称遵守本建议书提出的规范。

6 SDN功能架构概述

本节阐明使用SDN的、基于[ITU-T Y.3300]中SDN高层架构的安全业务（如，防火墙和DDoS攻击减缓）的高层参考架构，如，集中式防火墙业务和集中式DDoS攻击减缓业务。

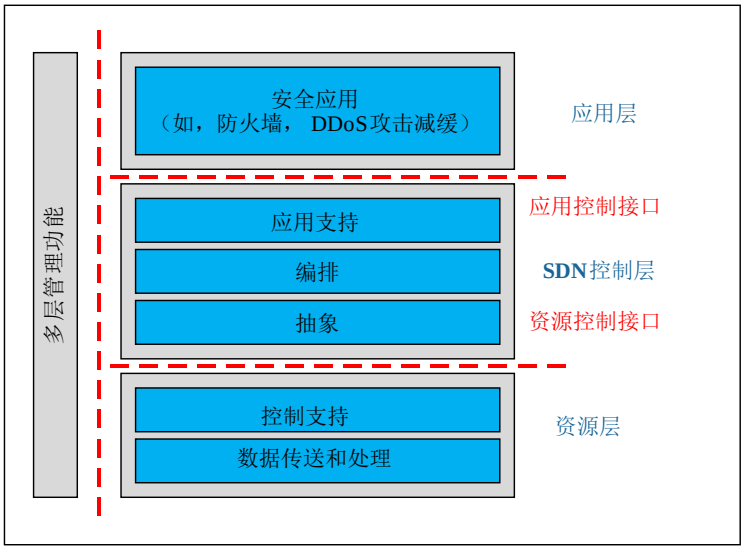


图6-1 – 基于SDN的安全业务的高层架构

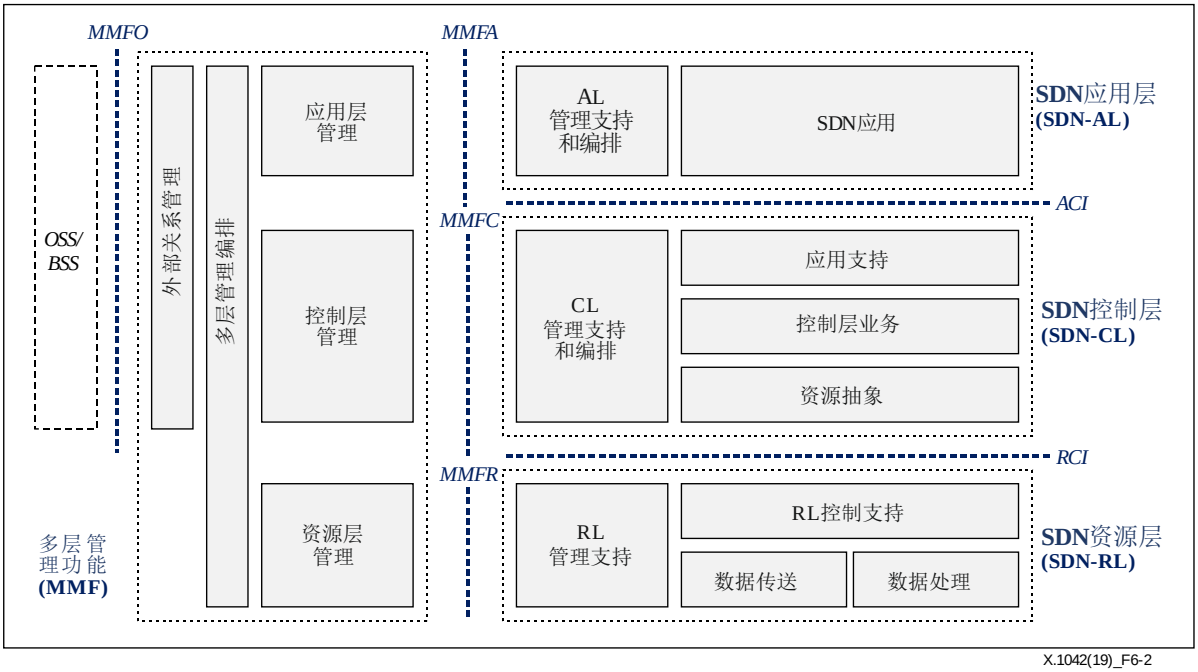
如图6-1所示，安全业务应用（如，防火墙、DDoS攻击减缓和蜜罐业务）在SDN架构顶端运行。当用户或管理员（如图6-2中的应用层管理（ALM））通过应用接口为安全业务执行安全政策时，SDN控制器产生相应的接入控制规则，以便以自主和迅速方式满足此类安全政策规定。根据所产生的接入控制规则，诸如SDN交换机等网络资源会采取行动缓解网络攻击，如丢弃具有令人生疑规律的数据包。

图6-2所示为[ITU-T Y.3302]中的SDN功能架构，这是基于SDN高层架构的。

– 软件定义网络应用层（SDN-AL）：SDN-AL包含ALM支持和编排（AL-MSO）功能成分和多个SDN应用功能成分[ITU-T Y.3302]。AL-MSO通过多层管理功能应用层（MMFA）参考点在多层管理功能（MMF）中与ALM功能成分互动，目的是支持SDN应用管理，并实现在所有SDN子层中的联合管理。SDN应用通过应用控制接口（ACI）参考点与软件定义网络 – 控制层（SDN-CL）互动，前者要求SDN-CL自动对网络资源的行为和特性进行量身定制。SDN应用使用网络资源的抽象视图和状态（这些由SDN-CL通过在ACI参考点上暴露的信息和数据模型提供）。根据SDN使用情况（如，数据中心、移动网络和接入网络内或之间），可以可选方式确定不同ACI。在此假设ACI使用开放应用程序接口。

– SDN-CL：SDN-CL包含控制层管理支持和编排（CL-MSO）、控制层应用支持（CL-AS）、控制层业务（CL-CLS）和资源抽象（CL-RA）。SDN-CL根据SDN-AL请求和MMF政策提供控制SDN资源（如数据传送和处理资源）行为的可编程手段。SDN-CL对由软件定义网络--资源层（SDN-RL）提供的资源进行操作，并向SDN-AL暴露网络抽象视图。SDN-CL利用MMF中的控制层管理（CLM）功能成分（利用多层管理功能控制层（MMFC）参考点）与使用资源控制接口（RCI）参考点的SDN-RL互动。它还与带有ACI参考点的SDN-AL互动。CL-MSO可请求MMF将一些管理功能下放。MMF通过MMFC参考点提供管理SDN-CL功能的一些功能性。

– SDN-RL：SDN-RL包含资源层管理支持（RL-MS）、资源层控制支持、资源层数据处理和资源层数据传送。物理和虚拟网络元素正是在SDN-RL处按照SDN-CL决定进行数据包的传送和/或处理。由于SDN-CL所做决定产生的政策调配信息（包括配置信息）以及关于网络资源的信息通过RCI参考点交换。通过RCI交换的信息包括由SDN-CL向SDN-RL提供的控制信心（如，配置网络资源或提供政策）以及当发现网络资源变化（如提供此类信息）时，涉及由SDN-RL所发通知的信息。RL-MS提供资源描述，即，厂商、软件版本及其现状（如，中央处理单元负荷、所用的随机存取内存内存或存储容量）。还可以包括进行某种本地管理工作的管理代理（如果由MMF下放）。MMF通过多层管理功能参考层（MMFR）参考点提供管理SDN-RL功能的功能性。



BSS：业务支持系统；MMFO：多层管理功能OSS/BSS；OSS：操作支持系统

图6-2 – SDN功能架构[ITU-T Y.3302]

7 网路资源分类

本节定义使用SDN的、基于图6-2的安全业务的四种网络资源：

1) SDN应用：这是一种通过北向接口（如图6-2的ACI）将其网络要求和所希望的网络行为向SDN控制器进行明确、直接和可编程沟通的业务。此外，SDN应用为了做出内部决策，可能会消耗网络抽象视图。例如，防火墙、蜜罐、DDoS减缓和非法装置管理业务可作为应用得到提供。这些SDN应用被要求通过AL-MSO与ALM互动，以便进行故障、配置、账户、性能和安全管理。另外这些应用都可制定接入规则，因此也要求它们通过ACI与SDN-CL互动，以使接入规则得到实施。

2) SDN控制器：一个逻辑上的集中式实体，负责：i) 将SDN应用要求进行转换并提供给SDN交换机；ii) 利用有益的网络信息，如流量统计数据和事件，为应用提供抽象网络视图。换言之，SDN控制器根据其从SDN应用那里获得的接入规则，创建流程条目（low entries），因此，要求SDN控制器与CLM、SDN应用和SDN-RL进行互动。

3) SDN交换机：可以是一个软件程序或硬件装置，在SDN环境中将数据包进行前传。SDN交换机能够通过南向接口（如图6-2所示的RCL）存储由SDN控制器管理的数字包前传规则，因此，要求SDN交换机与资源层管理（RLM）和SDN-CL进行互动。

4) 安全管理器（SM）：一种ALM功能，负责向SDN应用传送安全政策，因此，要求SM通过AL-MSO与SDN应用互动。图7-1所示为图6-2中网络资源的位置。要求这些网路资源遵守[ITU Y.3301]提出的要求。

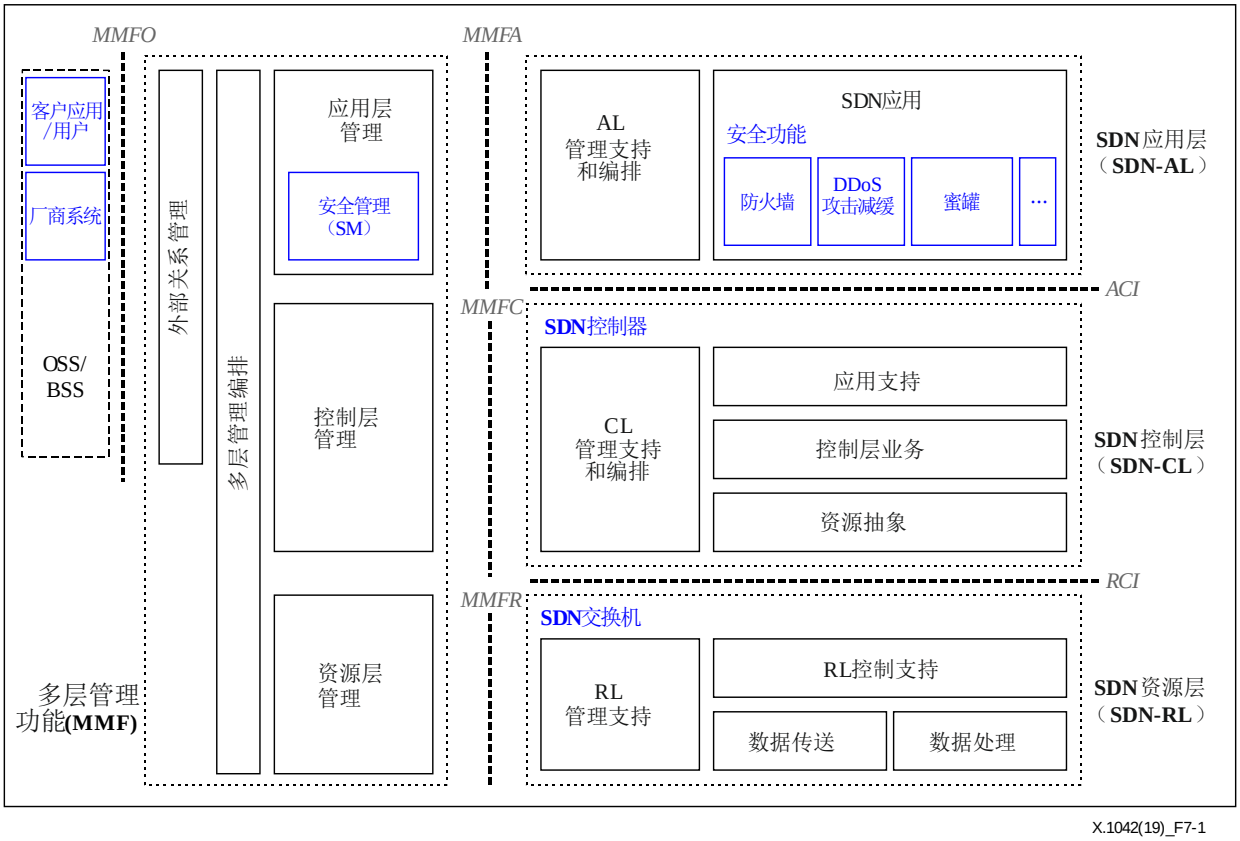


图7-1 – 基于SDN的安全业务的网络资源

8 基于SDN的安全业务

本节介绍两类网络中使用SDN的安全业务：i) 域内网络，如，集中式防火墙业务和集中式蜜罐业务；ii) 域间网络，如，集中式DDoS攻击减缓业务和集中式非法装置管理业务。本建议书所述域系指通过共同规则和程序管理的一组网络资源。

8.1 集中式防火墙业务

8.1.1 集中式防火墙业务的基本概念

本段阐述集中式防火墙业务的基本概念。该业务可对网络资源进行管理，从而使防火墙规则得到灵活管理。如图8-1所示，集中式防火墙对SDN交换机进行管理，因此，可在这些交换机上加入或取消规则。

注 – 通过控制器可以轻而易举地将防火墙应用发布的数据包过滤战略转换为流程表（flow table）。然而，目前控制器与交换机之间的协议（如开放流（OpenFlow）和网络配置协议（NETCONF））仅仅能够与传输控制协议（TCP）层匹配，不存在的相应的、设定TCP层之上数据包身份信息的字段。不改变现有协议将无法实现明确TCP层之上信息的防火墙战略。

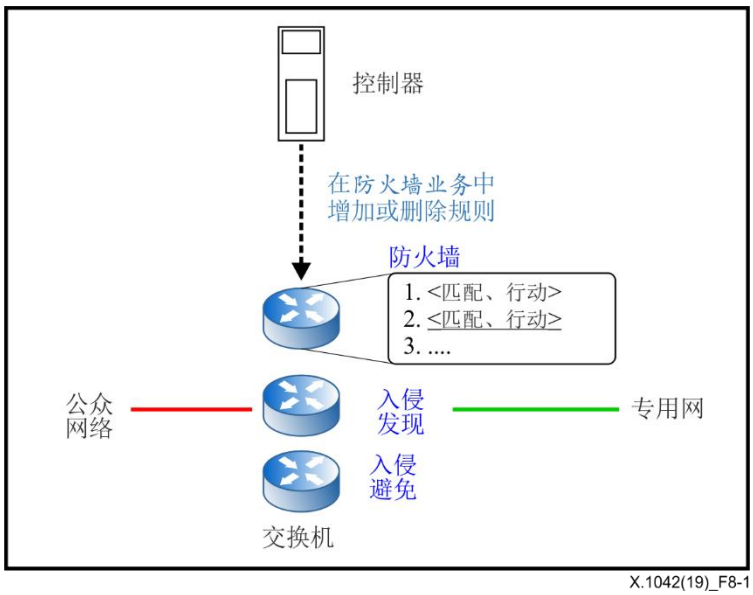


图8-1 – 集中式防火墙业务的概念

8.1.2 集中式防火墙业务的业务情形

图8-2所示为组织蠕虫病毒传播的集中式防火墙业务情形举例。

为这种情形的前提条件，SM应在发现有关新蠕虫病毒的信息时为防火墙应用规定新的政策。为了防止包含这种蠕虫病毒的数据包扩散，用户可以为运行在SDN控制器顶端的防火墙应用增加新政策（如，“丢弃带有蠕虫病毒文档的数据包”）。还可以对之进行集中管理，以便SM能够通过单一点，即SDN控制器，为防火墙应用确定安全政策。

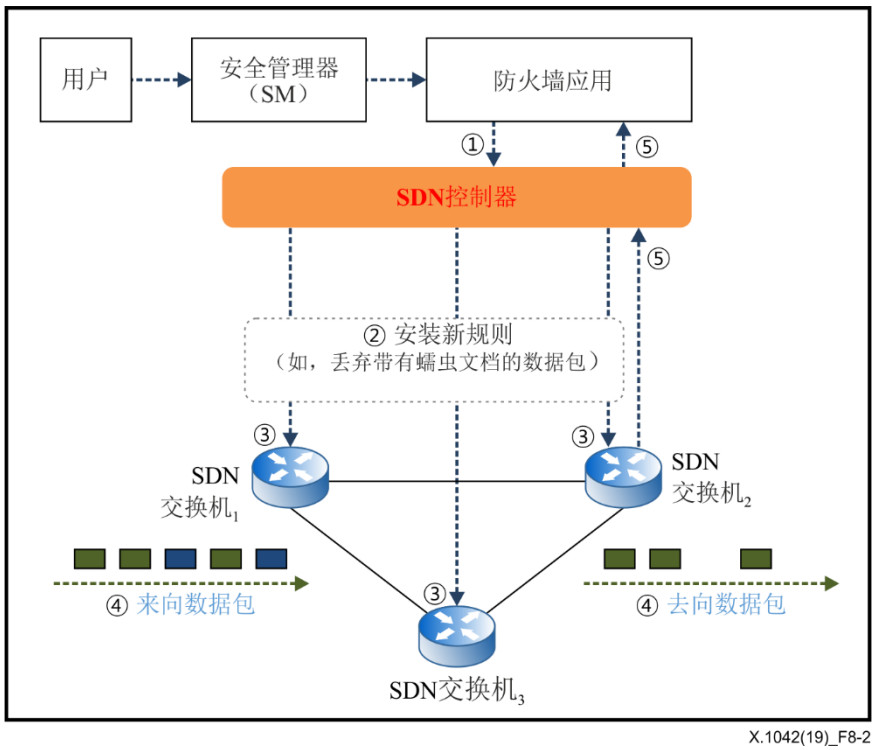


图 8-2 – 集中式防火墙业务的域内情形

– 步骤1：防火墙应用安装新规则。

防火墙应用应在得到有关新蠕虫病毒报告时规定新规则。该新规则（如，丢弃带有蠕虫病毒文档的数据包）被增加到SDN控制器上。

– 步骤2：SDN控制器向所有SDN交换机发布新的流程条目。

SDN控制器在安装后可将新的流程条目发布给每一交换机，因此，SDN控制器向所有SDN交换机发送包含规则（如，“丢弃带有蠕虫病毒文档的数据包”）的流程插入操作指令。

本节新报告的蠕虫或称作蠕虫或称作“零日”（zero-day）虫。对于已知蠕虫病毒，已在防火墙业务中开发了一些机制，如“签名”或“拇指指纹”，以发现和防卫蠕虫。然而，对于“零日”虫，则应在采取对之进行防卫的任何应对措施之前对之进行扫描和发现。蠕虫会提供恶意有效载荷，消耗了宝贵的应用或业务。可通过检查数据包有效载荷发现这些蠕虫病毒。附录II给出通过数据包数据扫描发现蠕虫的示例。

– 步骤3：所有SDN交换机都在其流程表中加入新的流程条目。

SDN交换机在收到有关蠕虫病毒文档的流程插入操作指令后，将“丢弃未来带有蠕虫病毒文档的数据包”这一流程条目增加到其流程表中。之后，SDN交换机可丢弃带有蠕虫病毒文档的数据包。

– 步骤4：SDN交换机执行丢弃带有蠕虫病毒文档数据包的流程条目。

SDN交换机在收到带有蠕虫病毒文档的数据包时完全丢弃这些数据包。按照已实施规则，任何带有蠕虫病毒文档的数据包都不可通过。

– 步骤5：SDN交换机在收到不熟悉的数据包时向控制器报告。

SDN交换机在收到某种其从未处理过的数据包时，会将该数据包删除，并将这类数据包情况向控制器报告。控制器做出分析，以确定这是否是一种攻击。如果是一种攻击，则控制器将信息发至防火墙应用，从而使步骤1得到执行。如果不是攻击，则控制器保持正常流动条目，以告诉交换机如何处理随后数据包的序列。

8.1.3 协助式防火墙业务的业务情形

图8-3所示为协作式防火墙应用的情形示例，其中带有深度数据包检查（DPI）应用，以实现集中式互联网协议语音（VoIP）/长期演进语音（VoLTE）的流程监督和管理。该情形表明，DPI应用通过以动态方式增加、删除或修改规则，控制每一SDN交换机的VoIP/VoLTE的呼叫流程管理。该应用可与防火墙应用合作，保护VoIP/VoLTE业务。具体而言，由防火墙促成的交换机对未知流程数据包进行基本安全检查。如果交换机检测到该数据包包含某种规律可疑的、VoIP未知呼叫流程数据包，则它会触发SDN控制器对这些可疑VoIP呼叫数据包专门安全分析。

作为这种情形的前提条件，SM应在发现有关可疑规律的信息时为防火墙和DPI应用规定新的政策。为了防止包含这种规律的数据包扩散，用户可以为运行在SDN控制器顶端的防火墙和DPI应用增加新政策（如，“丢弃规律可疑的数据包”）。还可以对之进行集中管理，以便SM能够通过单一点，即SDN控制器，为上述应用确定安全政策。

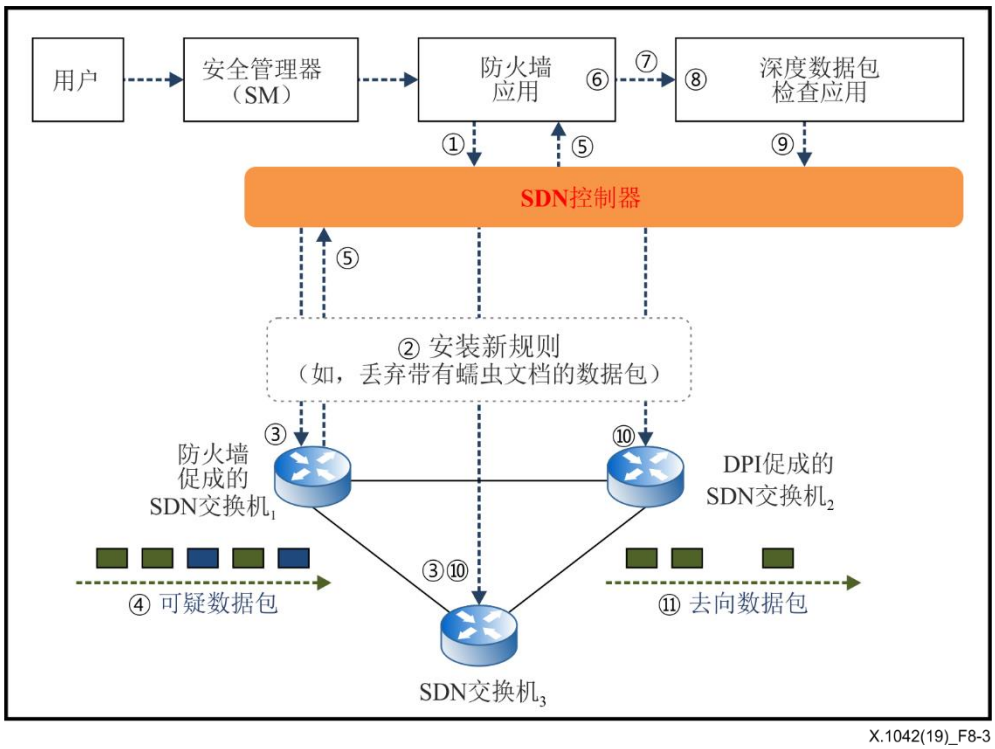


图8-3 – 协作式防火墙业务的域内情形

– 步骤1：防火墙和DPI应用为熟知规律安装新规则。

防火墙和DPI应用应在收到有关新规律报告时确定新规则。该新规则（如，将带有这一规律的数据包提供给SDN控制器）被增加到SDN控制器上。

– 步骤2：SDN控制器向所有SDN交换机发布新的流程条目。

SDN控制器可向每一交换机发布新的流程条目，因此，SDN控制器向所有SDN交换机发送包含规则（如，提交带有该规律的数据包）的流程插入操作指令。如果每一交换机都有不同功能，则SDN控制器为每一交换机发送一不同的流程条目。也就是说，由防火墙促成的交换机不应得到DPI相关流程条目。

– 步骤3：所有SDN交换机都在其流程表中加入新的流程条目。

所有SDN交换机都增加一条流程条目，以便在从SDN控制器那里收到流程插入操作指令时，将其流程表中的具有令人生疑规律的未来数据包予以交付。

– 步骤4：SDN交换机执行交付带有令人生疑规律数据包的流程条目。

SDN交换机在收到具有令人生疑规律的数据包时将数据包提供给SDN控制器。按照已实施规则，所有带有令人生疑规律的数据包都应传送至SDN控制器。

– 步骤5：SDN交换机和控制器在收到不熟悉数据包时将之前转给防火墙应用。

当SDN控制器收到某类此前从未处理过的数据包时，它将这些数据包前转至防火墙应用进行基本安全检查。

– 步骤6：防火墙应用分析不熟悉的数据包。

防火墙应用分析数据包的字头字段，并确定这是未知的VoIP呼叫流程信号数据包，例如，规律令人生疑的会话起始协议（SIP）数据包。

– 步骤7：防火墙应用触发DPI应用程序。

防火墙应用触发相关应用，如DPI应用，以详细分析可疑信号数据包的安全性。之后，它将数据包前转至DPI应用。

– 步骤8：DPI应用分析不熟悉的数据包。

DPI应用分析信号数据包的字头和内容，如主叫号码和会话描述字头。例如，如果DPI应用将数据包视为由黑客破坏过的数据包，或是为了寻找寻找VoIP/VoLTE装置而发送的扫描数据包，则将该数据包丢弃。

– 步骤9：DPI应用要求SDN控制器封堵该数据包。

DPI应用请求SDN控制器封堵该数据包以及具有相同呼叫识别符的随后所有数据包。

– 步骤10：SDN控制器安装新规则。

SDN控制器向所有SDN交换机发布新流程条目（如，“丢弃数据包”）（同步骤2）。之后，这些交换机将丢弃所有非法数据包。

8.2 集中式蜜罐业务

8.2.1 集中式蜜罐业务的基本概念

本段阐明集中式蜜罐业务的基本概念。蜜罐可以动态管理蜜罐的地点。如图8-4所示，集中式蜜罐管理交换机和新的路由路径，以便攻击者吸引到一个作为陷阱的地方，即蜜罐那里。蜜罐被配置为受攻击目标，并将收集到的信息向集中式蜜罐业务报告。

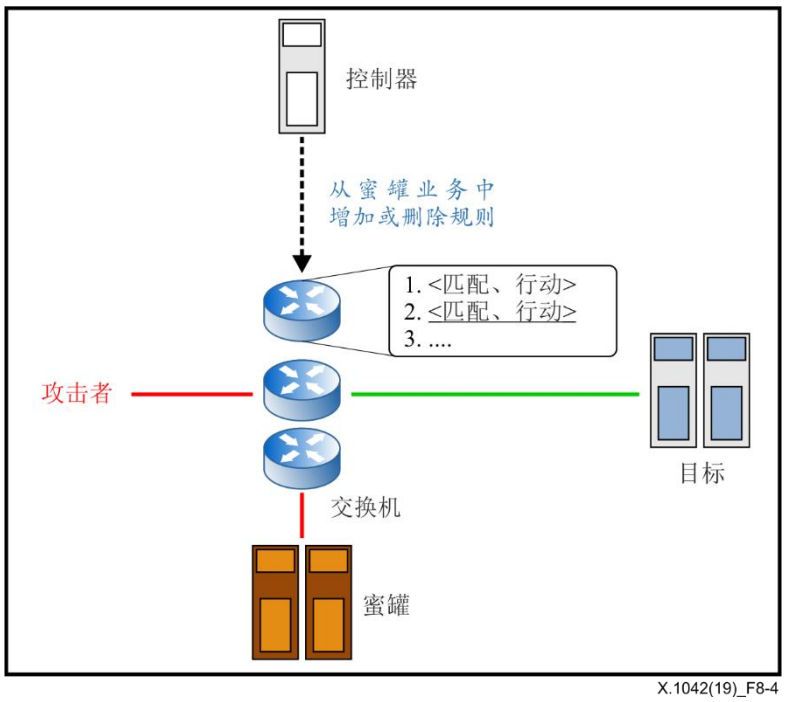


图8-4 – 集中式蜜罐业务的概念

8.2.2 集中式蜜罐业务情形

图8-5以示例说明集中式蜜罐业务情形，为蜜罐增加路由路径而非作为实际目标的SDN交换机。

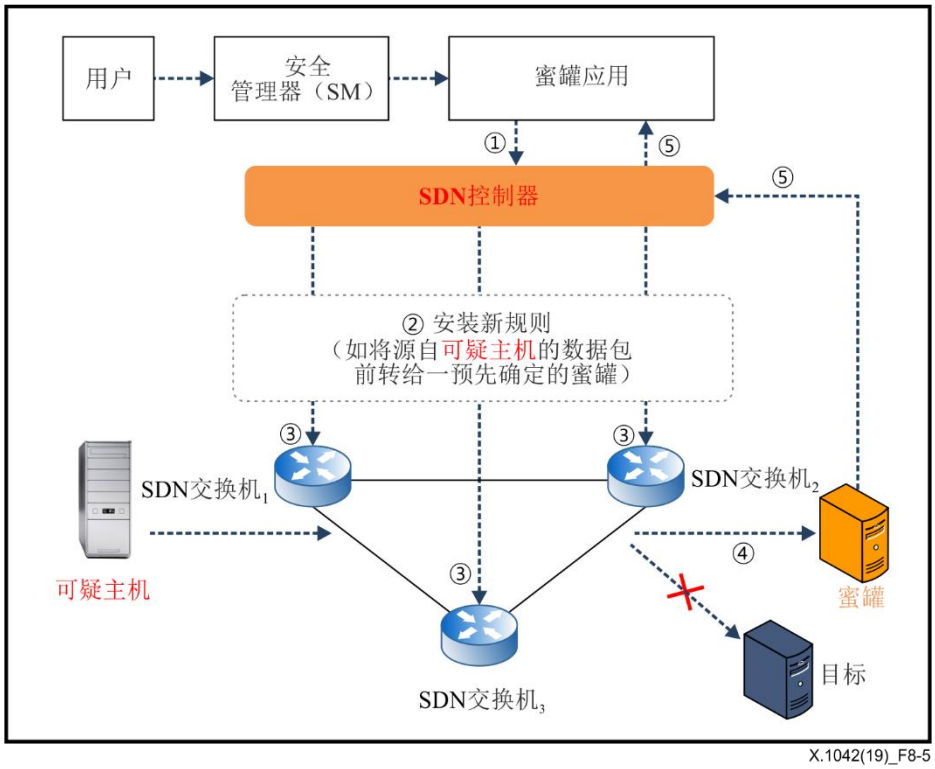


图8-5 – 集中式蜜罐业务的域内情形

– 步骤1：蜜罐应用在SDN控制器上安装新规则。

蜜罐应用在收到有关可疑主机的信息时应规定新的规则。为了监视来自可疑主机的流量，通过运行在SDN控制器顶部的蜜罐应用在SDN控制器上增加新规则（如，“将来自可疑主机的数据包前转至蜜罐”）。

– 步骤2：SDN控制器向SDN相关交换机发布新规则。

SDN控制器在安装新规则后可向每部交换机进行发布，因此，SDN控制器向所有SDN交换机发送含有规则（如，“将来自可疑主机的数据包前转至蜜罐”）的流程插入操作指令。还可进行集中管理，以便SM通过单一点，即SDN控制器，为其业务确定安全政策。

– 步骤3：所有SDN交换机都在其流程表中插入新规则。

所有SDN交换机都在其流程表中加入一条新的流程条目，当接收到有关可疑主机的流程插入操作指令时，将未来源自可疑主机的数据包前转至一蜜罐。之后，SDN交换可将源自可疑主机的数据包前转至蜜罐。

– 步骤4：SDN交换机执行旨在支持蜜罐业务的新规则。

SDN交换机在收到来自可疑主机的数据包时，可将其前转至蜜罐。按照已实施规则，任何源自可疑主机的数据包都不能通向实际的目标主机。得到前转的数据包在蜜罐中收集。

– 步骤5：蜜罐业务向控制器报告可疑数据包。

当蜜罐业务从可疑主机处收到数据包时，它对这些数据包进行处理，并向控制器发送有关这类数据包的报告，以支持控制器对数据包做出分析。

8.3 集中DDoS攻击减轻业务

8.3.1 集中DDoS攻击减轻业务的基本概念

图8-6显示了集中DDoS攻击减轻业务。该服务增加、删除或修改各SDN交换机的规则。与有关域内“集中防火墙业务”不同，该业务主要侧重于域间。

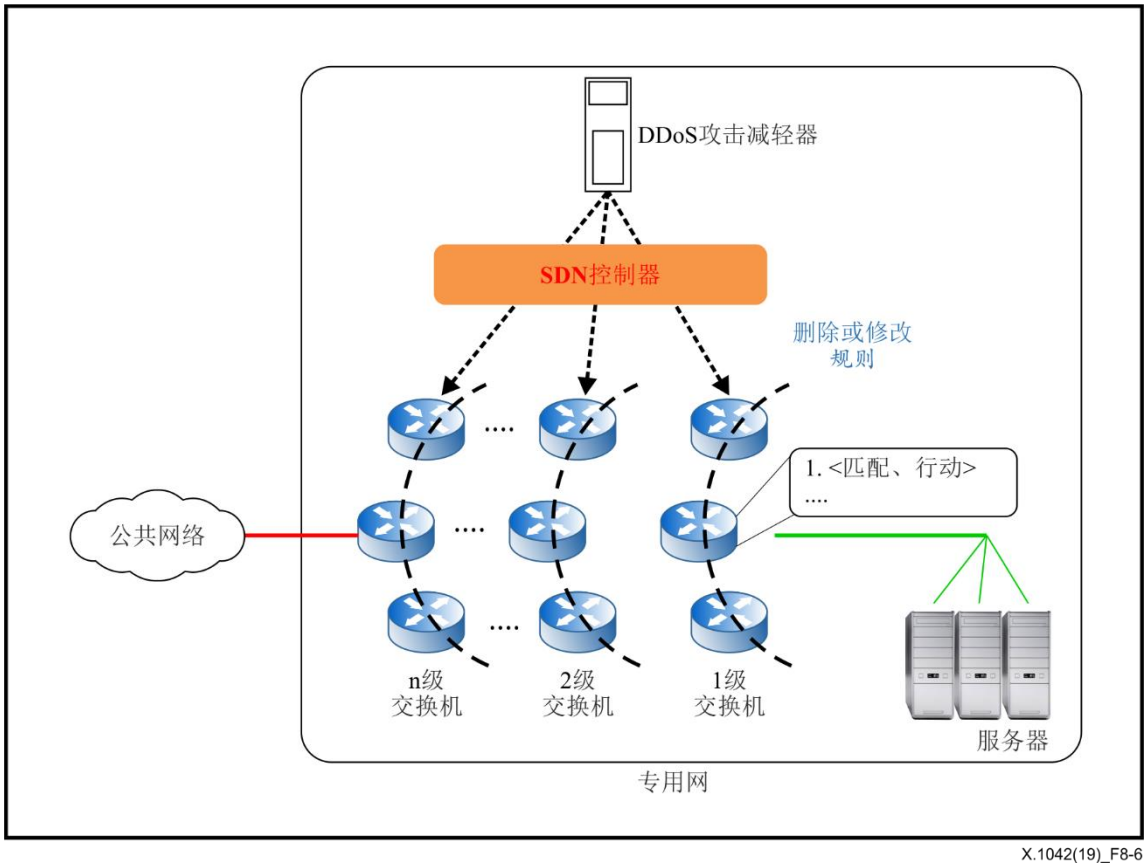


图8-6 – 集中DDoS攻击减轻业务概念

8.3.2 用于无状态服务器的集中DDoS攻击减轻业务

图8-7显示了用于无状态域名服务（DNS）服务器的集中DDoS攻击减轻业务情形示例。

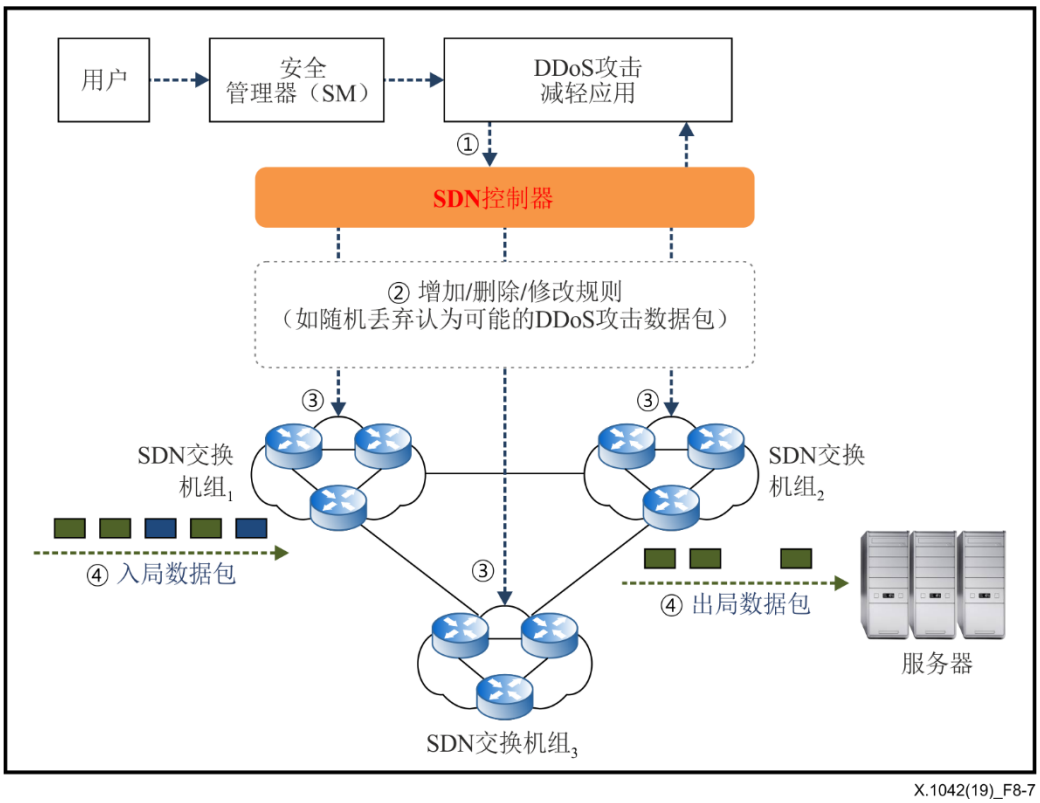


图8-7 – 用于无状态服务器的集中DDoS攻击减轻业务域间情形

– 步骤1：减轻应用为SDN控制器安装新的规则。

DDoS攻击减轻应用应在SM得知新的DDoS攻击时规定新的规则。为防止数据包到达服务器并造成服务器资源浪费，新的规则（如以一定概率随机丢弃DDoS攻击包）增加至SDN控制器。规则的增加是由运行在SDN控制器之上的DDoS攻击减轻应用进行的。

– 步骤2：SDN控制器为适当的交换机分配新的规则。

SDN控制器在安装后可能将规则分配至各交换机。因此，SDN控制器向所有SDN交换机发送包含规则（如以一定概率将所认为的DDoS攻击包随机丢弃）流插入操作。规则还可集中管理，使SM得以通过单点，即SDN控制器确定安全政策。

– 步骤3：所有SDN交换机在其流表内插入新的规则。

所有SDN交换机增加一个流条目，在收到有关DDoS攻击减轻的流插入操作时，向流表丢弃未来被视为DDoS攻击包的数据包。在此之后，域内交换机中的SDN交换机可按照与DDoS攻击严重度的相当概率丢弃DDoS攻击包。

– 步骤4：SDN交换机为减轻DDoS攻击执行新的规则。

SDN交换机在收到DDoS攻击包时有选择地完全丢弃数据包。DDoS攻击包按照各域的处理能力和域的特点通过各域内SDN交换机随机丢弃。在此之后，丢弃结果应报告SDN控制器。

8.3.3 用于有状态服务器的集中DDoS攻击减轻服务

图8-8显示了用于有状态网络服务器的集中DDoS攻击减轻情形示例。

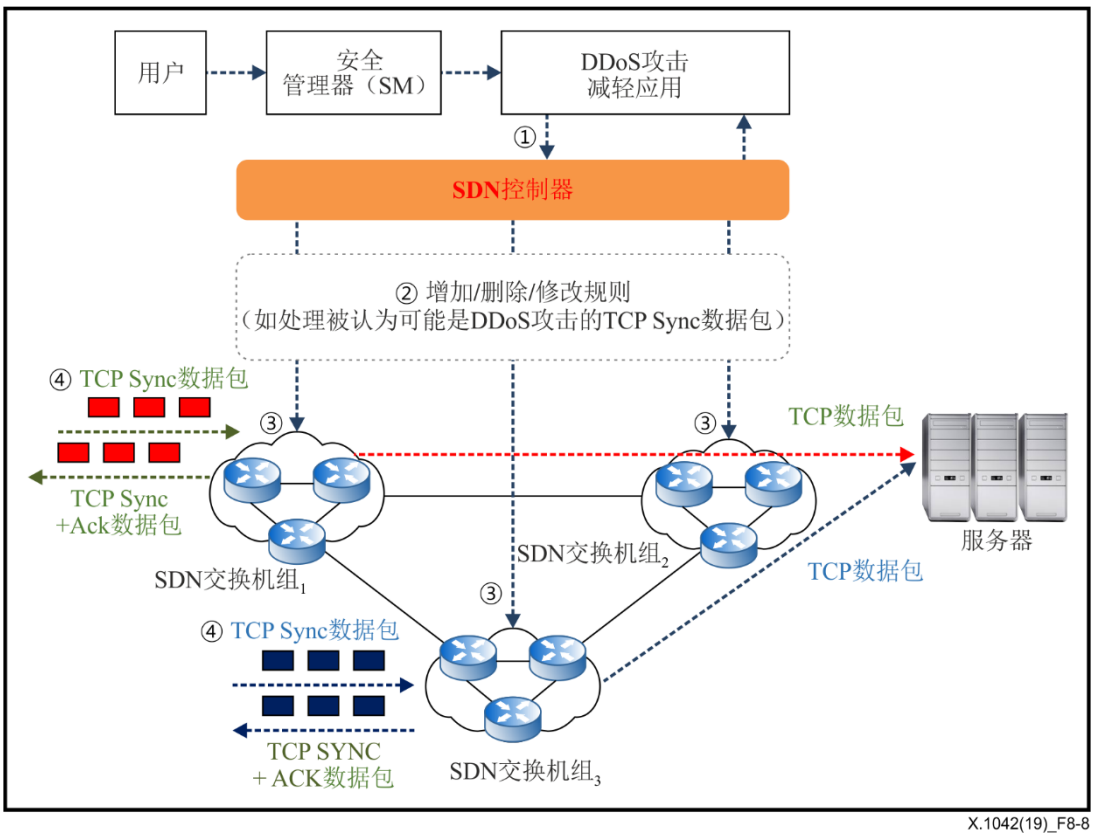


图8-8 – 用于有状态服务器的集中DDoS攻击减轻域间情形

– 步骤1：减轻应用为SDN控制器安装新的规则。

DDoS攻击减轻应用应选择由哪个交换机执行TCP服务代理规则。新规则的增加是由运行在SDN控制器之上的DDoS攻击减轻应用进行的。

– 步骤2：SDN控制器为适当的交换机分配新的规则。

SDN控制器在安装后可能会向适当的交换机分配新的规则，用于减轻DDoS攻击。因此，SDN控制器向所有SDN交换机发送包含规则（如“为被视为DDoS攻击的包生成TCP Sync+Ack”）的流插入操作。因此，新规则安装至所挑选的交换机，从而按请求为TCP同步生成TCP Sync-Ack。如同样的请求出现超过预期，SDN控制器选择新的交换机，使交换机作为服务器发挥作用。对于通常的TCP Sync，交换机将TCP会话传送至专用网的相应服务器。规则还可集中管理，使SM得以通过单点，即SDN控制器确定安全政策。

– 步骤3：所有SDN交换机在其流表内插入新的规则。

所有SDN交换机增加一个流条目，收到有关DDoS攻击减轻的流插入操作时，向流表丢弃未来被视为DDoS攻击包的数据包。在此之后，SDN交换机可以与DDoS攻击严重性相当的概率生成TCP Sync-Ack包。

– 步骤4：SDN交换机为减轻DDoS攻击执行新的规则。

SDN交换机在收到DDoS攻击包时对不良主机发出的TCP Sync包做出回应。DDoS攻击请求由交换机而不是实际的服务器处理有状态服务器。之后，SDN交换机的执行结果将用来减轻DDoS攻击并传送给SDN控制器。

8.4 集中非法装置管理业务

8.4.1 集中非法装置管理业务基本概率

该段描述了集中非法设备管理服务的基本概念。如图8-9所示，集中非法设备管理服务管理非法设备黑名单以防止这些设备的流量。非法设备名单保存在黑名单数据库中并可通过人工或自动方式由独立的应用进行更新。集中非法设备管理器定期从黑名单数据库加载非法设备清单并将事件报告给生成新的安全规则的非法设备应用，从而防止网络收到或发送流量至非法设备。

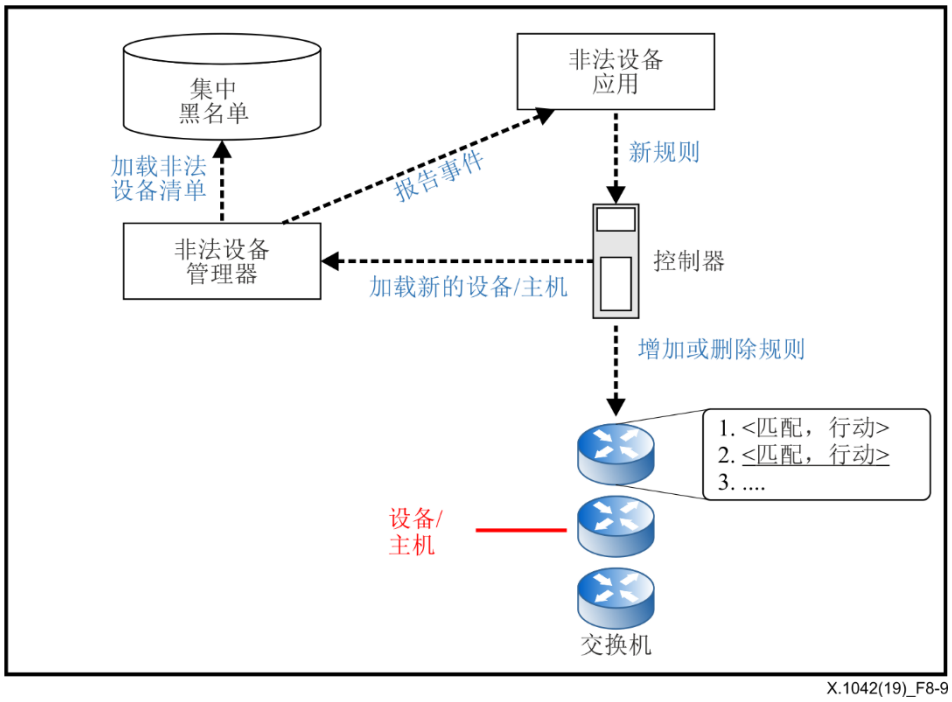


图8-9 – 集中非法装置管理业务概念

8.4.2 集中非法装置管理业务的业务情形

图8-10显示了集中非法设备管理服务的服务情形以防止被盗移动设备产生的流量。

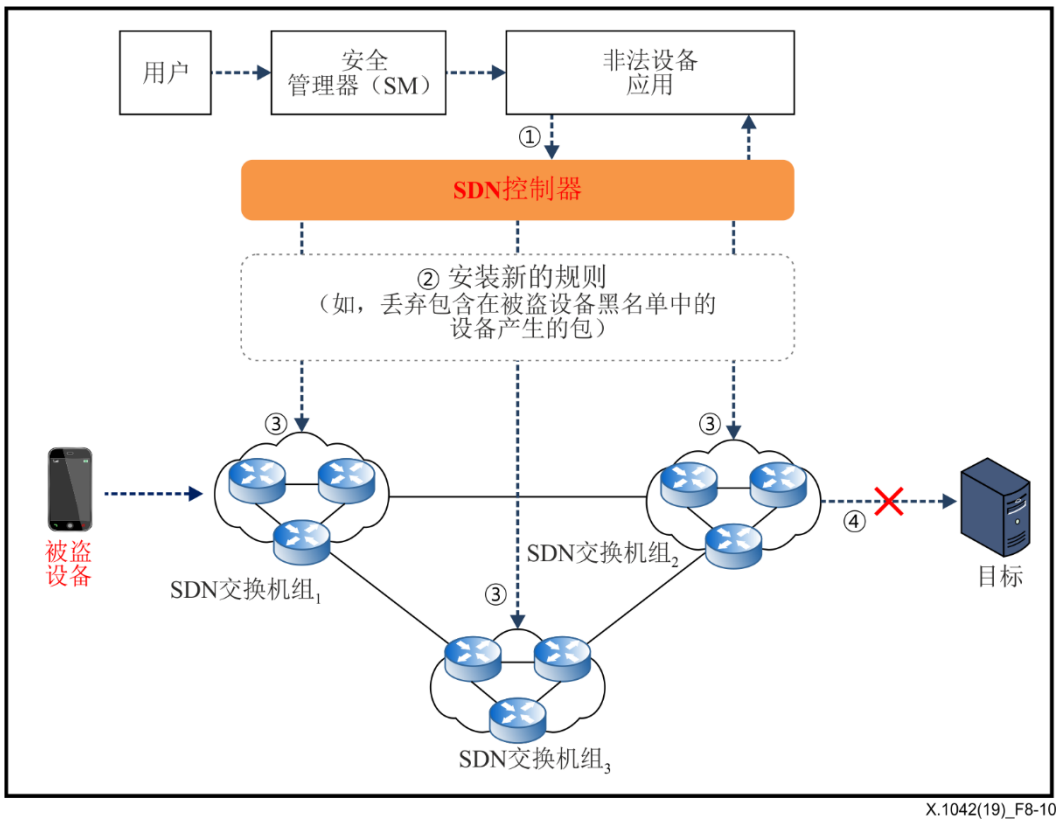


图8-10 – 集中非法装置管理业务域间情形

– 步骤1：非法设备管理应用安装新的规则

非法设备应用应在集中非法设备管理器报告了新的被盗设备信息时规定新的规则。作为这一情形的前提条件，非法设备应用或SM向SDN控制器增加新的规则（如“丢弃由保存在集中被盗设备黑名单中的设备产生的包。）

– 步骤2：SDN控制器分配新的规则

SDN控制器在安装后可能将规则分配至各交换机。因此，SDN控制器向所有SDN交换机发送包含规则（如，丢弃来自新的被盗设备的包）的流插入操作。规则还可集中管理，使集中非法设备管理器或SM得以通过单点，即SDN控制器确定安全政策。

– 步骤3：所有SDN交换机在其流表格中插入新的规则

所有SDN交换机增加流条目，在收到有关被盗设备插入操作信息时，丢弃从那些设备中产生的未来包。

– 步骤4：SDN交换机执行新的规则

SDN交换机在收到这些设备产生的包时完全丢弃这些数据包。任何由这些设备产生的数据包不得按照适用规则通过。在此之后，执行结果将传送SDN控制器。

注 – 重要的是，必须确定非法设备。集中非法设备管理器将使用独一无二的标识确定非法设备。如SDN控制器只识别网络地址，如该设备可动态变更的互联网协议（IP）地址和媒体接入控制（MAC）地址，则应安装新的规则，且应在非法设备网络地址每次修改时删除SDN控制器上的原有规则。

8.5 接入控制管理业务

8.5.1 接入控制管理业务的基本概念

该段阐述了接入控制管理（ACM）服务的基本概念。ACM模块利用SDN控制器可分层管理接入权政策。如图8-11所示，ACM模块管理接入权以防止对资源的非法接入。

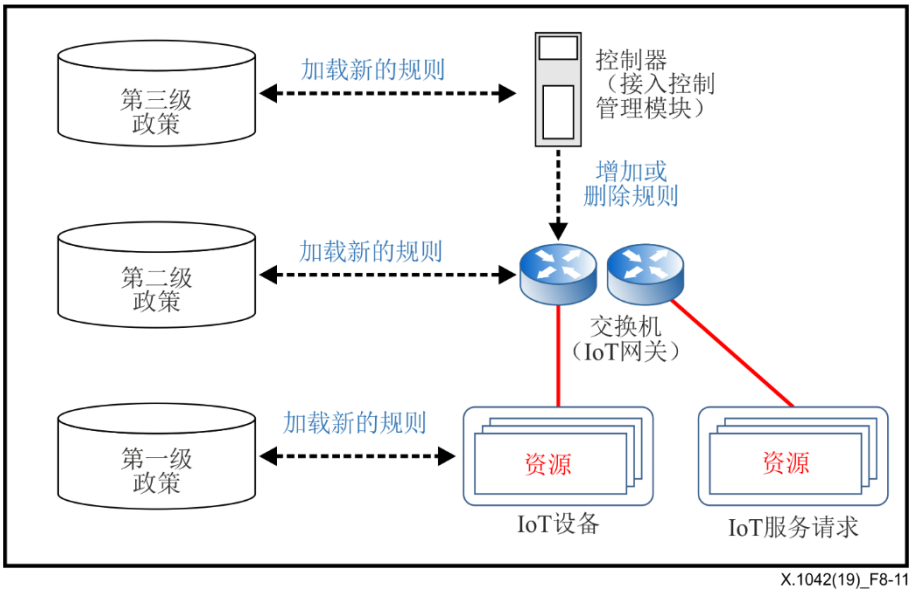


图8-11 – 接入控制管理业务概念

8.5.2 接入控制管理业务的业务情形

图8-12显示了由安全控制器管理的ACM服务的情形示例。该情形涉及SDN控制器和交换机两个方面。

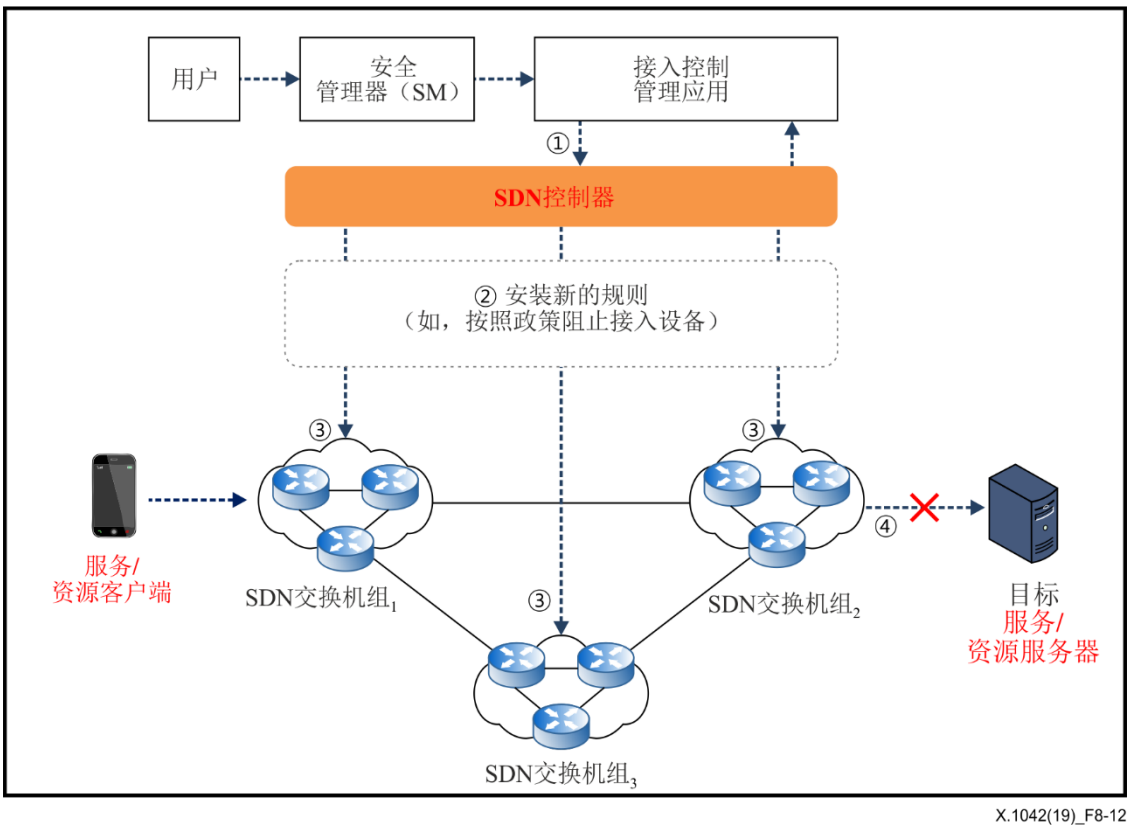


图8-12 – 接入控制管理业务的域间情形

– 步骤1：ACM从SM安装新的政策

ACM应用应规定接入分布式服务/资源设备的新政策（如IoT设备）。作为本情形的前提条件，SM已对ACM应用增加新的政策。

– 步骤2：SDN控制器分配新的规则

应保存新的规则。之后这些规则可通过SDN控制器分配至每个交换机。SDN控制器可发送接入请求，以便操作服务/资源设备中的资源。在此情况下，SDN控制器收不到SDN交换机用于分配规则的任何请求。SDN交换机在向SDN控制器发送规则分配请求前可要求SDN控制器服务/资源设备中的资源接入规则。

– 步骤3：所有SDN交换机应对其本地数据库增加新的规则

所有SDN交换机对其本地数据库增加新的规则以处理接入服务/资源设备的授权请求。

– 步骤4：SDN交换机执行新的规则

SDN交换机可在按照接入规则从服务/资源客户端收到包时完全丢弃这些包。在此，每个SDN交换机域应能根据各域的不同能力具有不同的接入规则。任何来自客户端的包无法根据适用规则利用SDN交换机通过。没有任何接入规则的包应报告给SDN控制器，以便由ACM应用进行管理。

附录 I

基于SDN的安全业务标准

（本附录并非此建议书不可分割的组成部分）

本附录为不同安全业务提供标准。

I.1 域内网络安全业务标准

I.1.1 集中防火墙业务

传统防火墙面临多项挑战，如高昂成本、性能、接入控制管理、政策制定和基于包的接入机制。为应对这些挑战，本建议书提出了基于SDN的集中防火墙服务。防火墙规则可通过集中服务器进行灵活管理。现有的SDN协议可通过防火墙应用和交换机之间的标准接口使用。

– 成本

为路由器、网关和交换机等网络资源增加防火墙的成本高昂，因为防火墙需要增加到每项网络资源。为解决这一问题，每项网络资源可以集中管理，从而集中服务器便可控制单一防火墙。

– 性能

防火墙的性能往往低于其网络界面的链路速度。每项网络资源有必要在不参考网络条件的情况下核对防火墙规则。防火墙可根据本框架中的网络条件通过调整予以部署。

– 接入控制管理

由于被管理的网络可能存在几百项网络资源，对像防火墙一样的安全服务接入控制的动态管理面临挑战。这是因为防火墙规则必须随着新的网络攻击的发生而动态增加。

– 政策的制定

每项网络资源都需要制定政策。然而，在特定的组织网络中，管理层难以确定允许哪些，拒绝哪些。因此，集中观看将有助于确定这类网络的安全政策。

– 基于包的接入机制

基于包的接入机制在现实中是不够用的，因为接入控制的基本单元往往是用户或应用。因此，管理者必须定义应用层面的规则并将其增加至防火墙服务。

I.1.2 集中蜜罐业务

传统蜜罐面临一些挑战，如高昂成本、性能、接入控制管理、政策的制定和基于包的接入机制。为应对这些挑战，本建议书提出了基于SDN的集中蜜罐服务框架。蜜罐可通过集中服务器进行灵活管理。现有的SDN协议可利用蜜罐应用和交换机之间的标准接口使用。

– 成本

在网络中运行附加的蜜罐成本很高，因为有必要使用蜜罐主机等网络资源。为解决这一问题，集中服务器可灵活管理蜜罐位置。

– 性能

蜜罐性能取决于主机能力。每个蜜罐总是以同样的方式运行，不参考网络或攻击条件。蜜罐可根据本框架内的网络或攻击条件通过调整予以部署。

– 接入控制管理

由于所管理的网络可能包含几百项网络资源，蜜罐的动态配置是一项挑战。这是因为，蜜罐位置需要为应对新的攻击而不断变更。

– 政策的制定

每项网络资源都需要制定政策。然而，根据网络和攻击条件，难以确定应对可疑攻击的具体蜜罐位置。因此，集中观看将有助于随着时间的流逝动态调整安全政策。

– 蜜罐部署机制

蜜罐位置应根据网络和攻击条件得到适当部署。基于SDN的集中蜜罐服务确定了优化监督位置并对攻击进行实时响应。蜜罐成为集中服务器集中配置的攻击对象。

I.2 域间网络安全业务标准

I.2.1 集中DDoS攻击减轻业务

集中DDoS攻击减轻服务取决于专用网以外（如公众网）针对DDoS攻击的服务器。服务器分为无状态服务器（如DNS服务器）和有状态服务器（如网络服务器）。图8-6显示了DDoS攻击减轻服务在专用网中的配置。专用网中交换机配置在不同域层面中，即1级交换机、2级交换机等。分层配置（Level-n）的交换机旨在动态防御各类DDoS攻击。

集中DDoS攻击减轻服务面对一些挑战，如高昂成本、性能、管理接入控制、政策制定和基于包的接入机制。为解决这些问题，本建议书提出了一个基于SDN的集中DDoS攻击减轻服务框架。DDoS攻击减轻规则可由集中服务器灵活管理。SDN协议可通过DDoS攻击减轻应用和交换机之间的标准接口予以使用。

– 成本

每项网络资源可以以最低的成本进行集中和灵活管理，使交换机能够由集中服务器在多个层面上予以配置和操纵。随着服务器DDoS攻击严重性的提高，多层交换机有选择地丢包以减轻DDoS攻击的影响。换言之，DDoS攻击可疑包将在通往受害主机的路径起点及早被丢弃。

– 性能

集中DDoS攻击减轻性能往往低于其网络接口链路速度。在传统服务中，每项网络资源需要在不考虑网络条件的情况下核对DDoS攻击减轻规则。然而，DDoS攻击减轻应用可根据本框架的网络条件经过调整得到部署。

– 接入控制管理

由于所管理的网络中可能有数百项网络资源，诸如DDoS攻击减轻这种安全服务的接入控制的动态管理是一项挑战。这是因为，DDoS攻击减轻规则需要针对新的DDoS攻击进行动态增加。

– 政策制定

每项网络资源都需要制定政策。然而，根据网络条件，难以确定应对DDoS攻击的具体丢包政策。因此，集中观看将有助于随时间的流逝动态调整安全政策。

– DDoS攻击检测机制

DDoS攻击的检测是通过检查来自客户端的服务请求是否在预期间隔内进入实现的。DDoS检测机制确定客户端请求是否为DDoS攻击的概率，从而按照概率更经常地进行选择性请求丢弃。

I.2.2 集中非法装置管理业务

传统非法设备管理服务面临一些挑战，如高昂成本、性能、接入控制管理、政策制定和基于包的接入机制。为应对这些挑战，本建议书提出了基于SDN的集中非法设备管理服务。可对将非法设备列入黑名单的规则进行全面管理。现有的SDN协议可通过非法装置应用和交换机之间的标准接口予以使用。

– 成本

更新路由器网关和交换机等网络资源黑名单的成本很高，因为有必要为每项单独的网络资源更新黑名单。为解决这一问题，可以对与各项网络黑名单相关的安全规则进行集中管理，使集中服务器可以操纵一个非法设备管理服务。

– 性能

由于来自黑名单所列设备的包在路径起点就已被丢弃，与传统管理服务不同，集中非法设备管理服务的性能在实际操作中得到改善。

– 管理接入控制

当在本地管理黑名单时，同步本地发布的黑名单并非轻而易举，因为不同国家可能有数百项网络资源，安全规则有必要针对新的非法设备动态添加。

– 政策制定

每项网络资源都需要制定政策。然而，在所管理的特定组织网络中，难以描述哪些设备不获准许。因此，集中观看将有助于确定这类网络的安全政策。

– 黑名单更新机制

维护和更新非法设备黑名单十分重要。因此，现有传统服务必须定期更新黑名单数据库，以便获得有关任何非法设备的最新信息。在集中非法设备管理服务中，黑名单是由集中服务器作为单一逻辑数据库集中管理的。

I.2.3 接入控制管理业务

ACM业务面临一些挑战，如高昂成本、性能、接入控制管理、政策制定和基于包的接入机制。为应对这些挑战，本建议书提出了基于SDN的ACM业务。可在分布式网络业务（如SDN控制器、交换机）中对将装置列入白名单的规则进行全面管理。现有的SDN协议可借助SDN控制器通过ACM应用和交换机之间的标准接口予以使用。

– 成本

更新路由器、网关和交换机等网络资源白名单的成本很高，因为有必要为每项单独的网络资源更新白名单。为解决这一问题，可以对与各项网络白名单相关的安全规则进行集中管理，使集中服务器可以操纵ACM业务。

– 性能

由于来自没有接入权装置的数据包在路径起点就已被丢弃，所以与传统管理业务不同，ACM业务的性能在实际操作中得到改善。此外，关于访问权限的信息将根据其安全级别划分并存储在网络资源中。

– 管理接入控制

当在本地管理白名单时，同步本地发布的白名单并非轻而易举，因为不同国家可能有数百项网络资源。安全规则有必要将新的接入权限动态传播至网络资源。

– 政策制定

应根据每项网络资源的安全级别制定器政策。然而，在所管理的特定组织网络中，难以按照ACM描述哪些IoT设备不获准许。因此，集中观看将有助于确定这类网络的安全政策。

– 白名单更新机制

维护和更新IoT装置接入权限白名单十分重要。因此，现有传统业务必须定期更新白名单数据库，以便保留有关任何IoT装置接入权限的最新信息。在ACM业务中，白名单是由集中服务器作为单一逻辑数据库集中管理的。此外，政策的一些部分可以分布到网络资源中。

附录 II

包数据扫描检测示例

（本附录并非此建议书不可分割的组成部分）

包数据扫描检测需要得到支持，以便检测并减轻蠕虫文件等攻击。管理者配置政策只能随机检测流内一些包，而不是所有包，以期实现更高性能。包数据扫描检测可采用的方案之一[b-ICIN SDNSec]涉及从每个流中挑选第一个m连续包以完成包数据扫描检测。该方案可针对所有流设计，或只针对满足某些条件的流设计，如来自某个IP地址源或通往某个目的地的包。

OpenFlow协议[b-ONF TS-012]，作为SDN南向接口实施方案之一，可进一步扩展，以便支持包数据扫描检测。在流条目格式中可增加另外两个功能。这些更新必须同时反映在控制器和交换机中。该方案的特点之一是包含包数据扫描检测的方案。另一项功能阐述了满足管理员或应用所配置的条件的流。之后，应在[b-ONF TS-012]第5.12节（见以下楷体案文）增加可选行动（OFPAT_DETECTION）：可选行动：检测行动将包前转至所规定的OpenFlow端口，然后到安全应用（如FW、IDP、DPI等）以用于进一步的数据扫描检测。这一新的行动类似于OpenFlow协议中的OFPAT_OUTPUT行动。最后，如以下楷体文字所示，[b-ONF TS-012]第7.2.4节的行动结构应更新。

```
enum ofp_action_type {
OFPAT_OUTPUT = 0,                                   /* Output to switch port. */
OFPAT_DETECTION = XX (a given number),      /*Output to switch port */
OFPAT_COPY_TTL_OUT = 11,      /* Copy TTL "outwards" – from
                                    next-to-outermost to outermost */
OFPAT_COPY_TTL_IN = 12,        /* Copy TTL "inwards" – from
                                    outermost to next-to-outermost */
OFPAT_SET_MPLS_TTL = 15,      /* MPLS TTL */
OFPAT_DEC_MPLS_TTL = 16,     /* Decrement MPLS TTL */
OFPAT_PUSH_VLAN = 17,         /* Push a new VLAN tag */
OFPAT_POP_VLAN = 18,          /* Pop the outer VLAN tag */
OFPAT_PUSH_MPLS = 19,         /* Push a new MPLS tag */
OFPAT_POP_MPLS = 20,          /* Pop the outer MPLS tag */
OFPAT_SET_QUEUE = 21,          /* Set queue id when outputting to a port */
OFPAT_GROUP = 22,              /* Apply group. */
OFPAT_SET_NW_TTL = 23,         /* IP TTL. */
OFPAT_DEC_NW_TTL = 24,          /* Decrement IP TTL. */
OFPAT_SET_FIELD = 25,           /*Set a header field using OXM TLV format*/
OFPAT_PUSH_PBB = 26,            /* Push a new PBB service tag (I-TAG) */
OFPAT_POP_PBB = 27,            /* Pop the outer PBB service tag (I-TAG) */
OFPAT_EXPERIMENTER = 0xffff
};
A Detection action uses the following structure and fields:
/*Action structure for OFPAT_DETECTION which sends packets out 'port'.*/
struct ofp_action_detection {
uint16_t type;                    /* OFPAT_DETECTION. */
uint16_t len;                     /* Length is 16. */
uint32_t port;                    /* Output port. */
uint16_t schema;                  /* One possible schema is: to select the first m
                                    consecutive packets from each flow. */
uint32_t condition;              /* One possible condition: packets
                                   of the flow to a certain destination . */
};
OFP_ASSERT(sizeof(struct ofp_action_output) == 10);
```

附录 III

基于SDN的安全业务架构实施

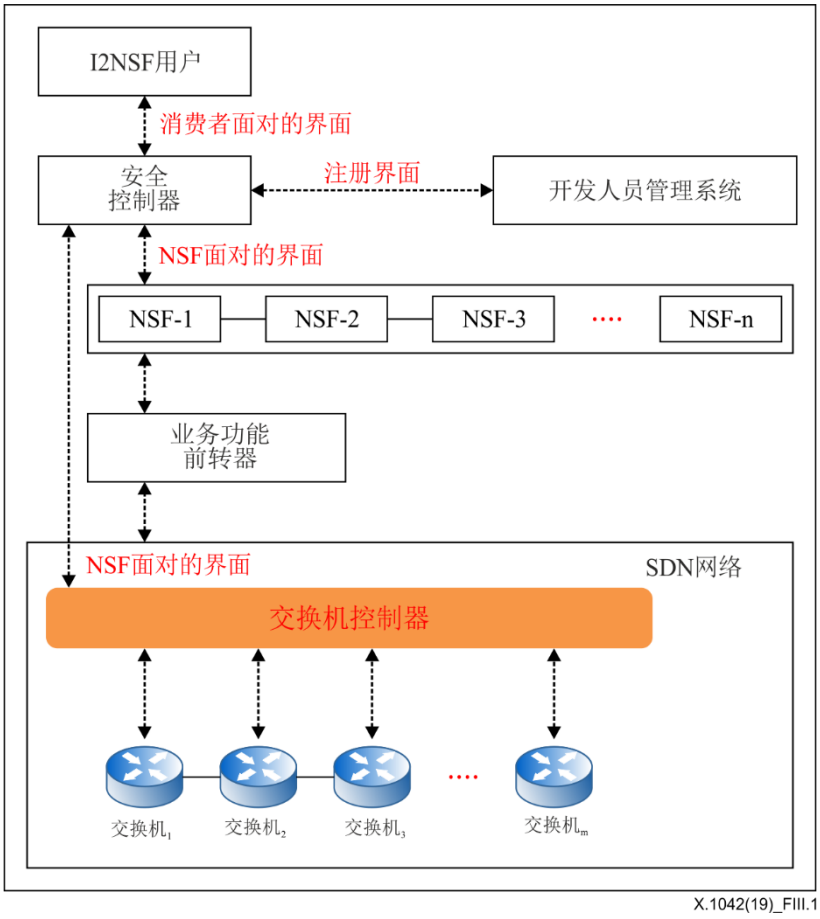
（本附录并非此建议书不可分割的组成部分）

III.1 IETF使用SDN的网络安全功能（I2NSF）框架界面

III.1.1 概况

本节为IETF提供了采用SDN的网络安全功能（I2NSF）框架界面，用于基于云的安全服务，如防火墙、DPI和DDoS攻击减轻功能。SDN通过控制其包前转规则实现在网络交换机中执行的包过滤。利用SDN能力优势，可以优化I2NSF框架中安全服务执行程序。

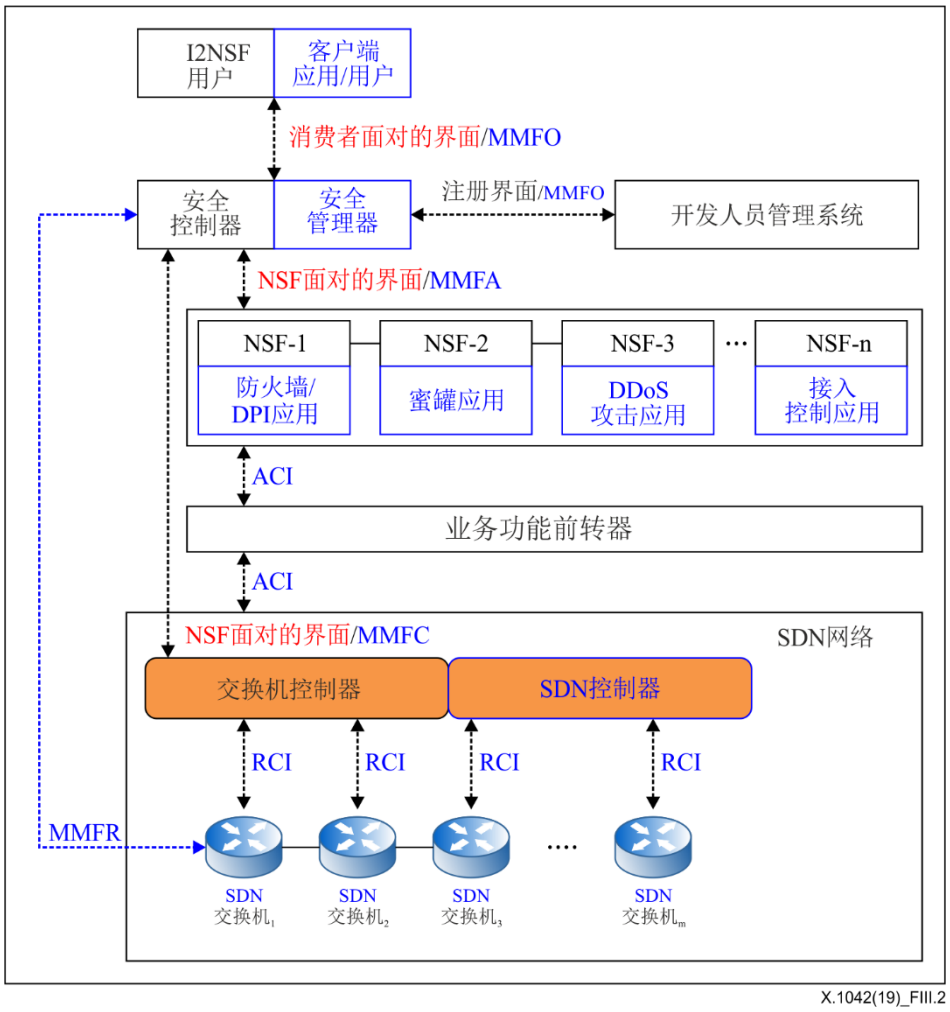
图III.1显示了使用SDN网络的I2NSF框架[b-IETF RFC8329]，用来支持基于网络的安全服务。在此框架中，安全政策规则的执行分为SDN交换机和网络安全功能（NSF）。在此，使用的是NETCONF协议和YANG建模语言。



图III-1 – IETF网络安全功能（I2NSF）框架界面

III.1.2 有关IETF和ITU-T架构的比较

图III.2显示了使用SDN的I2NSF框架和ITU-T架构之间的比较情况，ITU-T组件采用蓝色显示。

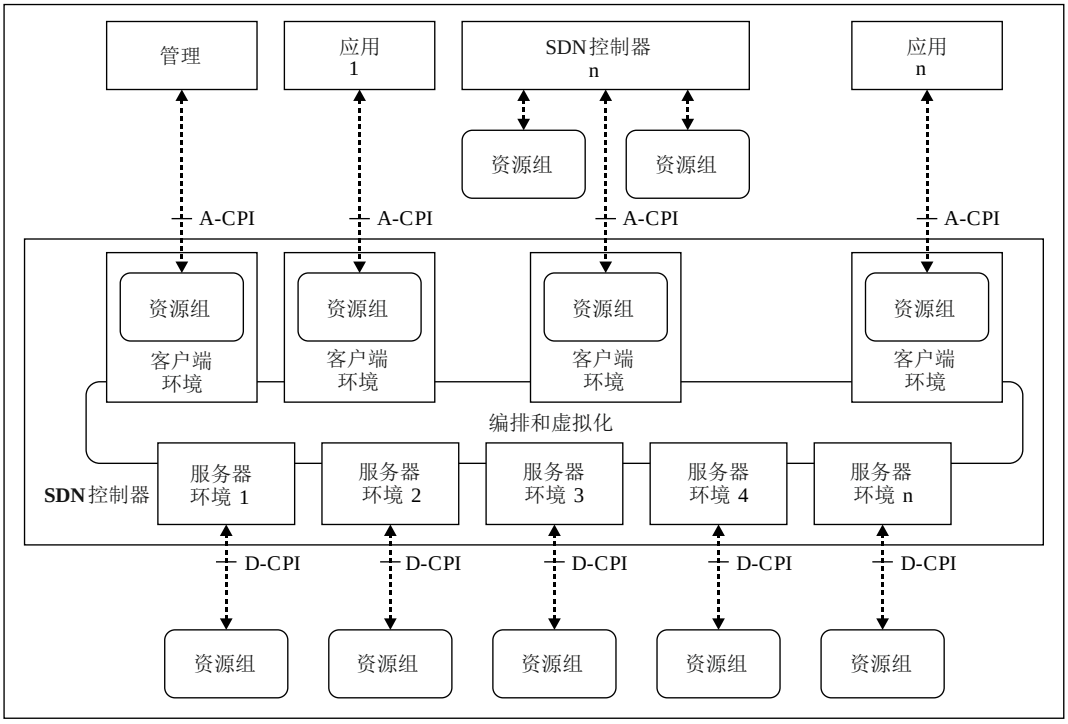


图III-2 – IETF和ITU-T架构比较

III.2 ONF中的SDN架构

III.2.1 概况

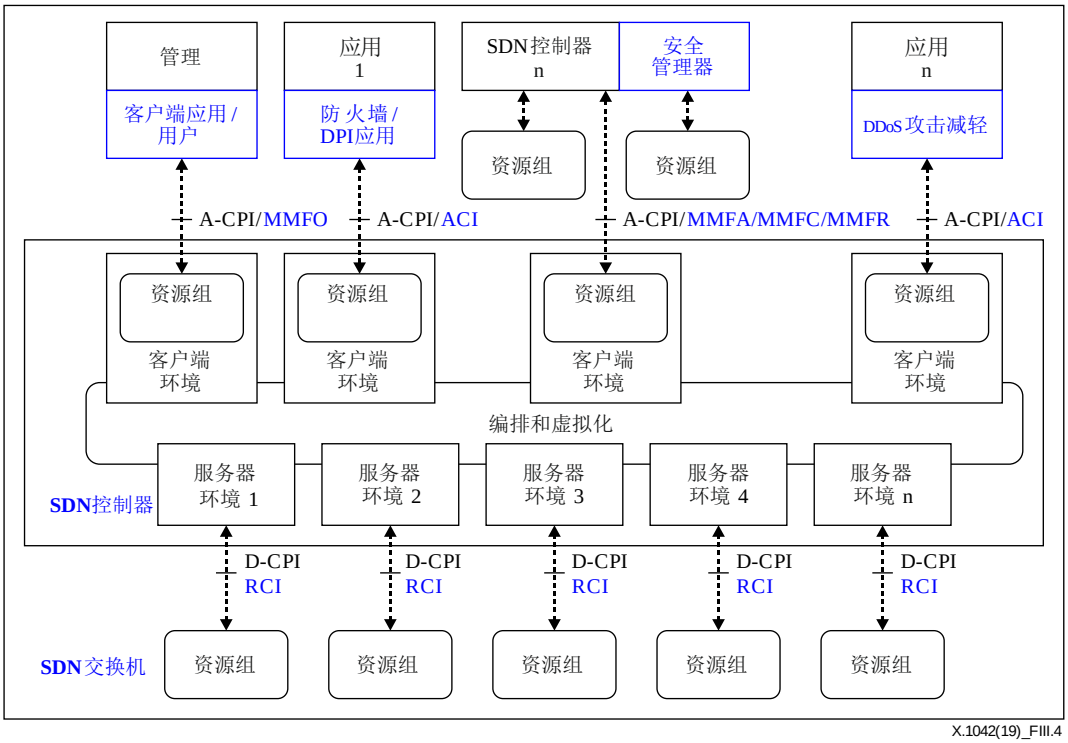
本节提供了ONF的SDN架构。图III.3显示了[b-ONF TR521]中的SDN架构。在图III.3中，SDN被建模为一组SDN控制器与其他本身可能作为SDN控制器的实体之间的客户端服务器关系。作为服务器，SDN控制器可向多个客户端提供服务，而作为客户端的SDN控制器则可从多个服务器中启动服务。只要它们显示出适当的界面行为，实体系内部细节中不属于SDN控制器的内容不在架构范畴之内。在此采用openflow协议。



图III-3 – ONF中的SDN架构

III.2.2 ONF和ITU-T架构的比较

图III.4显示了ONF和ITU-T架构的比较。ITU-T组件用蓝色显示



图III-4 – ONF和ITU-T架构的比较

参考文献

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ICIN SDNSec] Hu, Z., Wang, M., Yan, X., Yin, Y., Luo, Z. (2015). A comprehensive security architecture for SDN. In: *18th International Conference on Intelligence in Next Generation Networks*, pp 30-37. New York, NY: IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7073803

[b-IETF RFC 8329] IETF RFC 8329 (2018), *Framework for interface to network security functions*. https://tools.ietf.org/html/rfc8329.

[b-ONF TR-521] Open Networking Foundation TR-521 (2016), *SDN architecture*. https://www.opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf

[b-ONF TS-012] Open Networking Foundation TS-012 (2013). *OpenFlow switch specification V.1.4.0*.https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般关税原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2019年，日内瓦