使用NETCONF为防火墙下发安全策略（Python ncclient模块实现）

域间策略/安全域 NETCONF **胡伟** 2021-01-06 发表

组网及说明

设备：防火墙
型号：F1070
软件版本：D022及以上

说明：

- NETCONF（Network Configuration Protocol，网络配置协议）是一种基于XML的网络管理协议，他提供了一种可编程的、对网络设备进行配置和管理的方法。用户可以通过该协议设置属性、获取属性值、获取统计信息等。这使得他在第三方软件的开发上非常便利，很容易开发出在混合不同厂商、不同设备的环境下的特殊定制的网管软件。
- ncclient是一个用于NETCONF客户端的Python库。它旨在体用一个直观的API，将NETCONF的XML编码特性映射到Python构造和习语，并使编写网络管理脚本更容易。
  本次典型配置使用上述工具和组件为防火墙下发：**禁止源地址为1.1.1.1的安全策略。**
  【附】
  H3C Netconf配置相关指导
- **使用NETCONF配置设备操作指导书**
- Comware 7 NETCONF XML API Reference(请拨打400售后获取）。

配置步骤

1，确保Python以及ncclient库已成功安装，安装操作指导可参考相关网上链接。以下操作无报错说明ncclient库已安装成功。

```
C:\Users\Administrator>
C:\Users\Administrator>python
Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:57:54) [MSC v.1924 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> from ncclient import manager
>>>
>>>
```

2，明确脚本下发步骤。使用NETCONF为防火墙下发安全策略主要有以下四步（通过查看API文档分别找出每一步相关模块XML格式）：

- 创建IPv4地址对象组

XML structure

```
<OMS>
  <IPv4Groups>
    <Group>
      <Name></Name>
      <Description></Description>
      <SecurityZone></SecurityZone>
    </Group>
  </IPv4Groups>
</OMS>
```

- 创建IPv4地址对象

XML structure

```
<OMS>
  <IPv4Objs>
    <Obj>
      <Group></Group>
      <ID></ID>
      <Type></Type>
      <SubnetIPv4Address></SubnetIPv4Address>
      <IPv4Mask></IPv4Mask>
      <StartIPv4Address></StartIPv4Address>
      <EndIPv4Address></EndIPv4Address>
      <HostIPv4Address></HostIPv4Address>
      <HostName></HostName>
      <NestedGroup></NestedGroup>
      <VRFName></VRFName>
    </Obj>
  </IPv4Objs>
</OMS>
```

- 创建安全策略规则

XML structure

XML编写之前需要仔细阅读API文档，明确XML中 Table和Columns的定义和参数说明。

```
<SecurityPolicies>
  <RuleList>
    <Rule>
      <ID></ID>
      <RuleName></RuleName>
```