

Hillstone[®]
防火墙技术
StoneOS安全模式

山石网科通信技术(北京)有限公司
www.hillstonenet.com

Hillstone防火墙技术

StoneOS安全模式

1. 介绍

传统防火墙通常可以在两种模式下进行操作：NAT/路由模式和透明模式。NAT/路由模式部署灵活，并且支持防火墙和路由器两种设备的功能。尽管如此，许多希望通过最少的网络中断而实现安全保护的客户却会选择透明模式。随着二层与三层转换的扩展，安全集成到网络中变成一个更加困难的选择。那么，在哪里部署能够控制所有二层和三层的所有类型流量的安全功能呢？Hillstone的StoneOS提供了一个强大的安全平台，它为安全管理者提供了“集成安全控制和网络管理的底层网络结构”。

StoneOS通过将网络功能从安全功能中分离出来，扩展了NAT/路由模式。这样，用户就可以在一个完全灵活的环境下使用NAT功能。

StoneOS通过引入专有的Virtual Switch（虚拟交换机）的概念极大地扩展了透明模式。在二层，用户可以定义VLAN域，并且可以将不同的安全策略应用到每一个VLAN。StoneOS还拥有重新标记VLAN tag功能，这种功能只有高端的交换机才能实现。

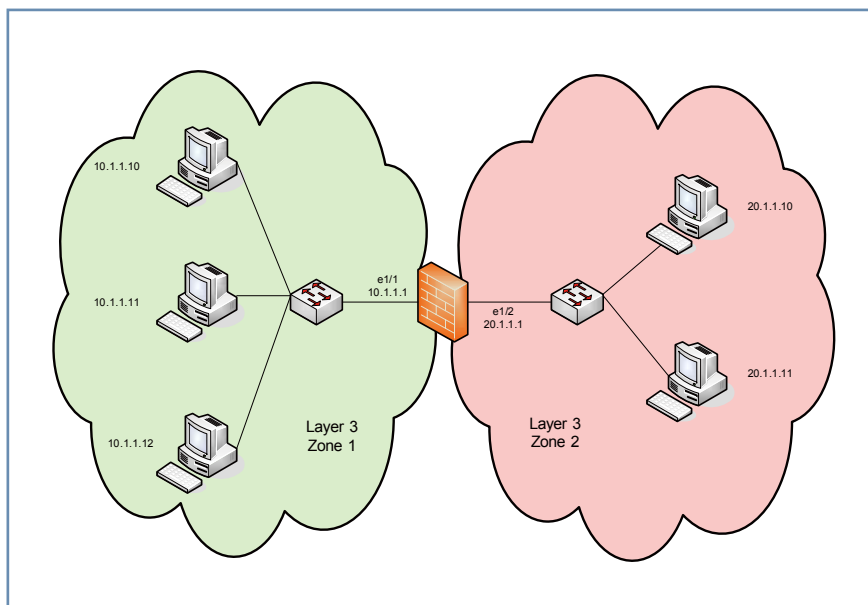
StoneOS混合模式将NAT/路由模式与透明模式结合到同一个设备上。根据配置的安全策略，部分数据在二层进行处理，而其它数据进行三层处理。这个强大的功能将路由器和交换机的功能进行完美结合，并且能够降低网络部署的复杂性。

2. NAT/路由模式路由

在NAT/路由模式下，设备被划分为多个三层域。流量会在三层域之间进行转发，并且被转发的流量会被进行安全检查。对于路由模式，IP地址不会被转换。对于NAT模式，IP数据包在不同域间转发的过程中，其IP地址和端口号可以被转换。

Hillstone设备将安全管理从网络管理中分离出来。Hillstone NAT策略是网络管理的一部分，用户可以基于特定接口或者五元组（IP地址、端口号和服务）进行灵活配置，或者将两者相结合。Hillstone设备可以同时工作在路由模式和NAT模式下，即对一些数据做三层转发的同时，为另外一些数据做NAT转换。

图1: NAT/路由模式部署 ▶



StoneOS支持:

源NAT:

- 接口IP, IP地址池
- NAT和NAPT
- Sticky功能
- 特定类型流量 – IP五元组匹配(源和目的IP地址、端口号和服务)和出接口

目的NAT

- IP地址映射
- IP地址/端口号映射
- IP地址范围转换
- 负载均衡
- 特定类型流量 – IP五元组匹配(源和目的IP地址、端口号和服务), 可同时转换源地址、端口以及目的地址、端口

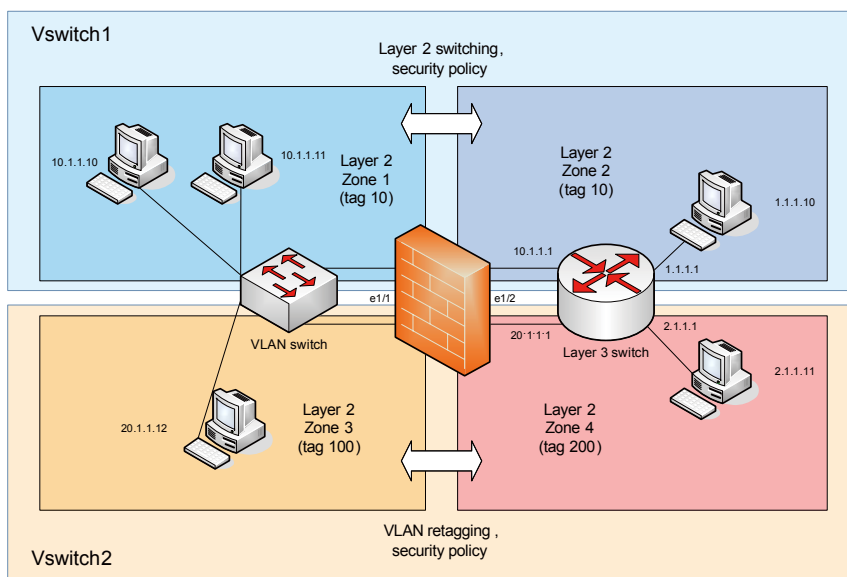
3. 透明模式

在透明模式下, 安全设备作为一个二层设备工作。IP层数据包头通常不会产生变化。如果得不到数据包的目的地址, 设备会将数据包转发到应用了安全策略的所有接口上。StoneOS通过VSwitch概念形成虚拟广播域。

StoneOS安全设备能够部署到复杂的VLAN环节中, 在执行细粒度安全检查和过滤的同时不改变底层网络配置或者拓扑。

3.1 虚拟交换机 (Virtual Switch)

图2: StoneOS透明模式和VSwitch ▶



一个VSwitch是一个VLAN广播域。一个VSwitch包含一个或者多个VLAN子接口。子接口通常都使用相同的VLAN标签。例如，在图2中，e1/1的VLAN10和e1/2的VLAN10属于同一个VSwitch。在Zone 1和Zone 2之间，可以配置策略规则来控制流量的传输和执行流量的安全检查。如果策略允许，标签为10的流量就能够在域之间传输。

一个VSwitch中也可以包含具有不同VLAN标签的子接口。在这种情况下，StoneOS除了在域之间传输流量（如果策略允许），还可以对VLAN进行tag的重新标记。图2的VSwitch2显示了VLAN重新标记tag功能。

3.2 StoneOS透明模式

StoneOS的二层转发是在VSwitch中完成的。一个VSwitch中包含了一个或者多个二层域，而这些二层安全域依次包含了VLAN子接口。二层域之间定义了策略规则来控制访问和过滤流量。在透明模式下，主接口（无标签）和子接口都没有配置IP地址。

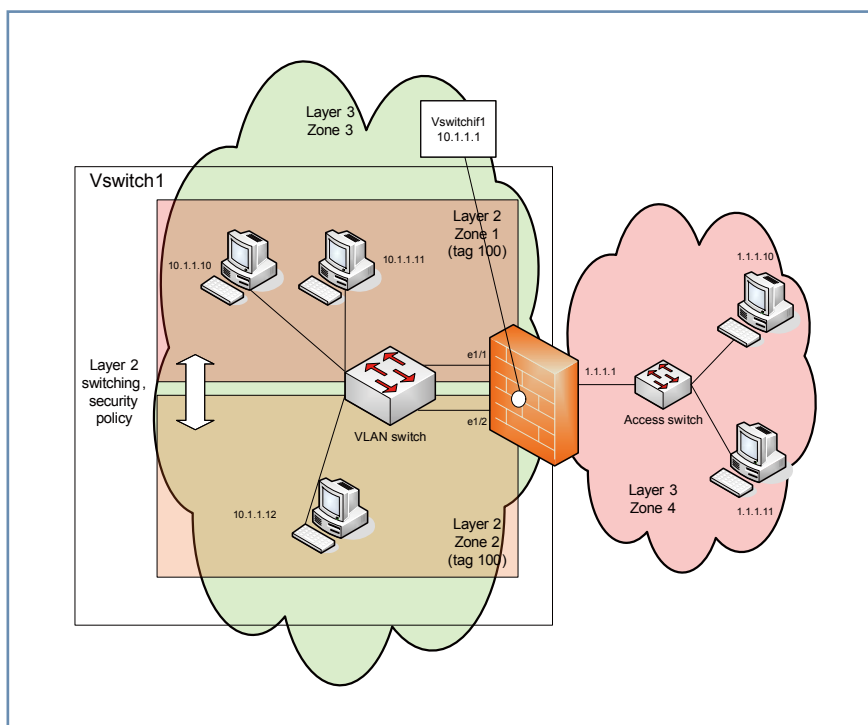
StoneOS有一个预定义的VSwitch，即VSwitch1。默认情况下，预定义二层域都被绑定到VSwitch1中，而且，如果策略允许，无标签流量会根据配置在二层域之间和内部进行交换。

StoneOS在接口上执行MAC学习，从而降低广播需求。

4. StoneOS混合模式

StoneOS的数据平面将NAT/路由模式以及透明模式无缝结合在一起。一个单一的NAT/路由模式或者单一的透明模式的产生是因为没有另一个模式的操作。在StoneOS中，混合模式（NAT/路由模式与透明模式的联合模式）是天然形成的。

图3: StoneOS混合模式 ▶



在图3的例子中，一个VSwitch中有一个（可能是多个）VLAN。标签为100的VLAN有两组用户，分别是Layer 2 zone 1中的“Students”和Layer 2 zone 2中的“Teachers”。在透明模式下，这两组用户可以通过配置策略规则互相访问。例如，我们可以允许“Teachers”访问“Students”的机器，但是不允许“Students”访问“Teachers”的机器。二层域之间的通信通过交换完成。这就是系统的透明模式。

在图3的示例中，我们还有一组服务器，地址为1.1.1.1/24。“Students”和“Teachers”需要通过路由访问这些服务器。在StoneOS中，用户可以创建一个虚拟的三层接口，即为该例中的vswitchif1接口。这个三层接口有IP地址（10.1.1.1），并且可以作为“Students”和“Teachers”的网关。

用户可以为vswitchif1所在的域（名为zone3的三层域）和服务器所在的域（名为zone4的三层域）创建策略规则。这两个域之间的流量会被路由传输或者NAT传输。这就是系统的NAT/路由模式。

5. 结论

通过安全与路由交换的完美结合，StoneOS将安全与网络设备的集成提高到了一个新的高度。Hillstone通过对安全和网络功能的模块化管理扩展了传统的NAT/路由模式，允许复杂环境下的NAT配置。VSwitch概念在VLAN级别上实现细粒度安全策略，由此极大加强了透明模式的操作能力。

总而言之，Hillstone的混合操作模式开创了将交换机功能与路由器功能集于同一个设备的先河。混合操作模式使Hillstone安全设备可以取代多设备的联合使用，包括二层交换机、三层交换机、路由器和防火墙，由此极大地简化了网络的管理，降低网络方案的总体拥有成本，对用户投资实现了有效的保护！



山石网科通信技术(北京)有限公司

www.hillstonenet.com

北京总部

地 址: 北京市海淀区上地七街1号
汇众大厦3层
邮 编: 100085
电 话: +86(10)8289 7229
传 真: +86(10)8289 9814

上海办事处

地 址: 上海市陕西北路1388号
银座企业中心1721室
邮 编: 200060
电 话: +86(21)6149 8205
传 真: +86(21)6149 8001

成都办事处

地 址: 成都市总府路2号
时代广场A座26层2625
邮 编: 610016
电 话: +86(28)6606 7115
传 真: +86(28)6606 7199

广州办事处

地 址: 广州市天河区天河路208号
粤海天河城大厦13层1363室
邮 编: 510620
电 话: +86(20)2826 1950
传 真: +86(20)2826 1999

服务热线: 400-650-0259

Copyright © 2008, Hillstone Networks, Inc. 版权所有，保留所有权利。

Hillstone Networks、Hillstone Networks标识、Hillstone、Hillstone标识、StoneOS、StoneManager、Hillstone SA-2003、Hillstone SA-2005、Hillstone SA-2010、Hillstone SA-5020、Hillstone SA-5040、Hillstone SA-5050、Hillstone SR-330、Hillstone SR-530和Hillstone SR-550为Hillstone公司的商标。所有其他商标和注册商标均为本公司的财产。

本文所包含信息可能会有所修改，恕不另行通知。