

# StoneOS Security Modes

## 1. Introduction

There are generally two modes in which traditional firewalls can operate under: NAT/Route mode and transparent mode. NAT/Route mode offers the flexibility of deployment and can offer both the functionality of a firewall and a router. Still, a lot of customer who want to have security implemented with the least disruption to the network will opt for transparent mode. With the proliferation of Layer 2 and Layer 3 switches, security integration into the network becomes an even harder choice. Where do you deploy the security functionality which will have flexible control over both Layer 2 and Layer 3 traffic of all kinds? Hillstone Networks' StoneOS is a powerful security platform that offers security administrator the ability to integrate the security control and network management while maintaining the underlying network infrastructure.

StoneOS extended Route/NAT mode by separate network functionality from security functionality. As a result, NAT can be defined in a completely flexible way. The Route/NAT is one single mode inside Hillstone devices.

StoneOS greatly extended the transparent mode by introducing patent pending Virtual Switch (vswitch) concept. VLAN domain can be defined and difference security policies can be applied for each VLAN on layer 2. Furthermore, StoneOS vswitch also support VLAN retagging that can only be found on high end switches.

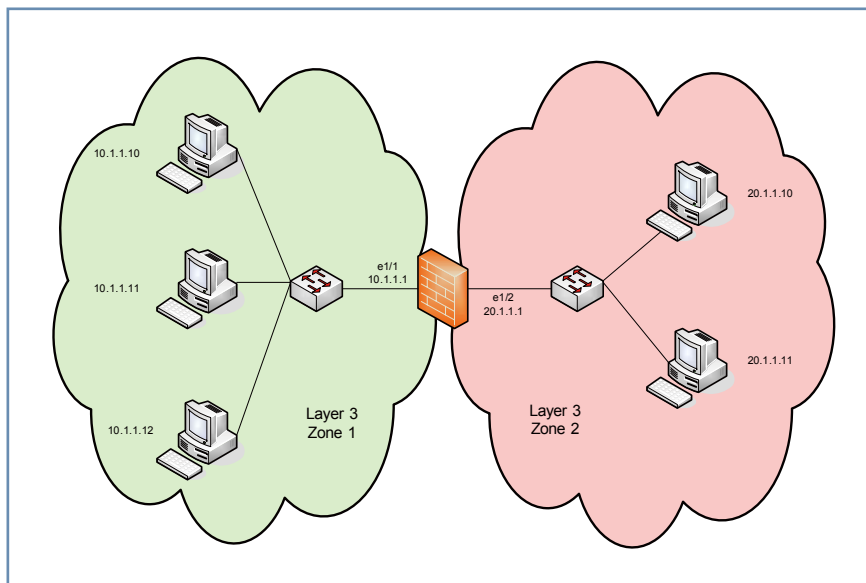
StoneOS mixed mode security which combines NAT/Route mode and transparent mode in one device. Part of the data traffic will operate in Layer 2, while other traffic operates in Layer 3, with security policy applied at both levels. This powerful functionality can be used to integrate router/switch functionality and reduce the complexity of network deployment.

## 2. Route/NAT mode

In Route/NAT mode, the device is divided into several layer 3 zones. Traffic will be routed between the layer 3 zones and security inspection will be performed on the traffic. For route mode, no address translation is performed on the IP packets. For NAT mode, additional address and port translation will be performed on the IP packets passing between the zones.

Hillstone devices separate security management from network management. Hillstone NAT policy is part of network management and can be flexibly configured on specific interface or based on 5-tuple (IP addresses, ports and service), or both. Hillstone devices can be in Route mode and NAT mode at the same time, route some traffic while doing NAT for other traffic.

Figure 1: Route/NAT mode deployment ▶



### StoneOS supports:

- Source NAT
- Interface IP, IP pool
- NAT and NAPT
- Sticky IP address
- Specific kind of traffic – IP 5-tuple match (source and destination addresses, ports, service) and egress interface

### Destination NAT

- IP address mapping
- IP address/port mapping
- IP range translation
- Load balancing
- Specific kind of traffic – IP 5-tuple match (source and destination addresses, ports, service) and ingress interface

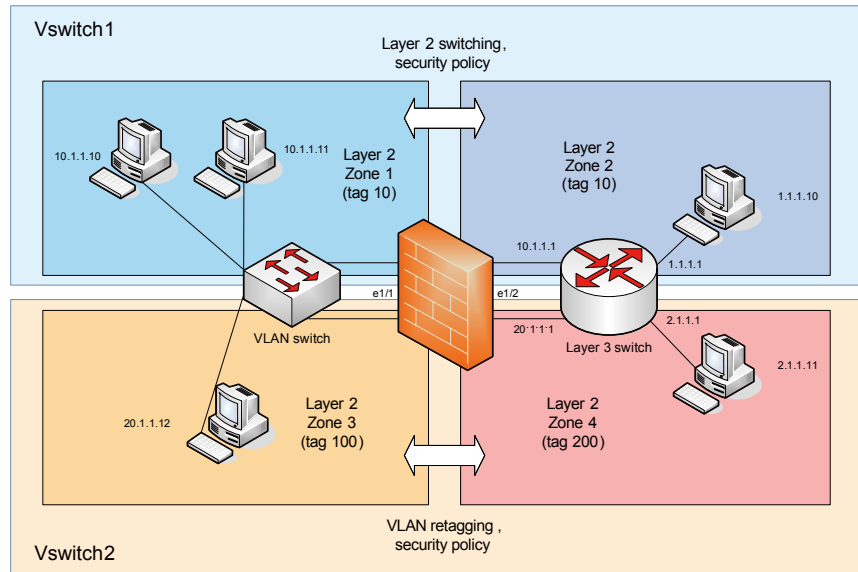
## 3. Transparent Mode

In transparent mode, the security device acts as Layer 2 device. The IP layer header is usually not changed. If destination of the packet is not known, the packet will be forwarded to all interfaces that the security policy

applies. StoneOS introduces Virtual Switch concept which virtualize the domain of the broadcast.

StoneOS security devices can be dropped in complex VLAN scenarios and perform fine grain security inspection and filtering without changing the underlying network configuration or topology.

Figure 2: HSOS Transparent mode and VSwitch



### 3.1 Virtual Switch

A vswitch is a VLAN broadcast/retagging domain. A vswitch consists of one or more of VLAN subinterfaces. The subinterfaces are usually with the same VLAN tag. For example, in Figure 2, VLAN 10 on ethernet1/1 and ethernet1/2 belong to the same VSwitch. Policy can be configured between Zone 1 and Zone 2 to control and perform security inspection on the traffic. If policy allows, tag 10 traffic will be switched between the zones.

A vswitch can also contain VLAN subinterfaces with different VLAN tags. IN this case, beside switching the traffic between the zones (if policy allows), VLAN retagging will also be performed. The VSwitch2 in Figure 2 shows such a scenario with VLAN retagging.

### 3.2 StoneOS Transparent Mode

Layer 2 forwarding of the StoneOS is limited inside a Virtual Switch. A virtual switch contains one or more Layer 2 zones which in turn hold the VLAN sub interfaces. Security policies are defined between the Layer 2 zones to control access and filter traffic. In transparent mode, the main (untagged) interfaces and subinterfaces do not have IP configured.

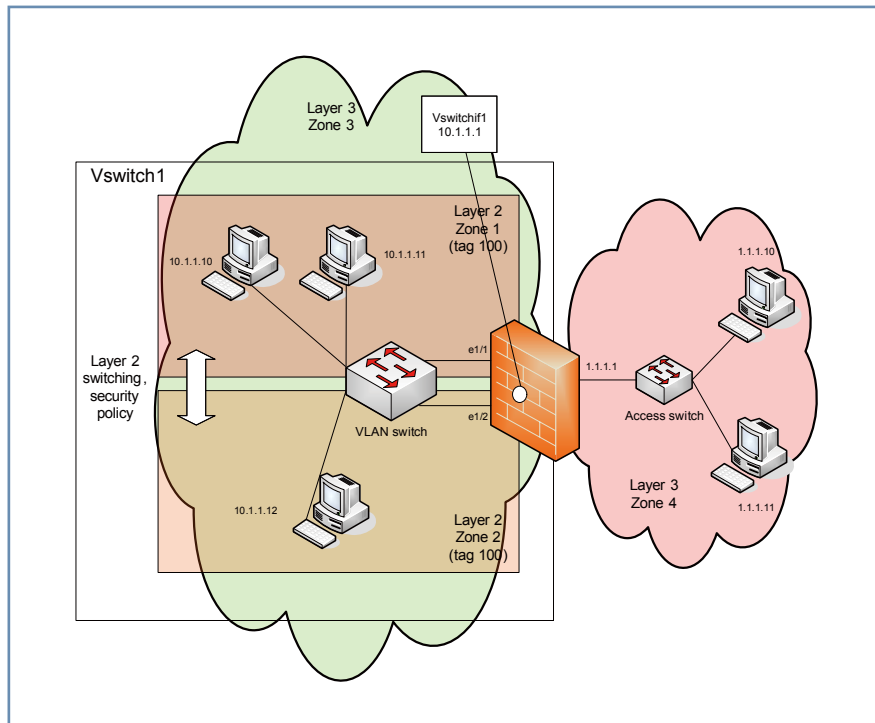
StoneOS has a predefined Virtual Switch: VSwitch1. By default, the predefined Layer 2 zones are in VSwitch1 and the configuration will switch untagged traffic within and between layer 2 zones if permitted by policy.

StoneOS perform MAC learning on interface ports to cut down on the need of broadcast.

#### 4. StoneOS Mixed Mode

StoneOS data plane combines Route/NAT mode and transparent mode seamlessly. A specific system is in pure Route/NAT mode or pure transparent mode simply because there is no part of the system operating in other modes. Mixed mode (combination of Route/NAT and transparent mode) is built in naturally in StoneOS.

Figure 3: StoneOS mixed mode operation ▶



In the example shown in Figure 3, we have one (of possibly many) VLAN in a Virtual switch. The VLAN of tag 100 have two group of users, 'Students' in Layer 2 zone 1, 'Teachers' in Layer 2 zone 2. As in transparent mode, these two groups of users can communicate with each other provided there are policies configured between the two zones. For example, we can allow teachers to access students' computer but not the other way around. The communication between Layer 2 zones is through VLAN switching and this is the transparent mode part of the system.

In this example, we also have a group of servers 1.1.1.0/24. To access these server, traffic from students' and teachers' computers need to be routed. In StoneOS, a virtual Layer 3 interface can be defined, in this case, vswitchif1. This layer 3 interface has IP (10.1.1.1) and can be a gateway for the students' and teachers' computer.

Security policies can be defined between the zone that vswitchif1 is in (a layer 3 zone called zone3) and the zone where the servers are in (a layer 3 zone called zone4). The traffic between these zones will be routed and or NAT'd and this is the Route/NAT part of the system.

## 5. Conclusion

By integrating security with switching, routing. StoneOS brings security and network integration to a new level. Hillstone Networks extended the traditional Route/NAT mode with modular management of security and network features, allow the ability of NAT configuration in very complex scenarios. Virtual Switch concept allows fine grain security policy on the per VLAN level, greatly enhance the capability of transparent mode operation.

Finally, Hillstone Networks introduces Mixed Mode operations that pioneers the integration of switching and routing functionality in the security device. This makes the device capable of replacing a combination of Layer 2 switches, Layer 3 switches, routers and firewalls at the same time, greatly enhance the network manageability and reduce the TCO of the network solution.