# Firewall Configuration Guide, Addendum 1801

November 2018

Supporting AT&T Vyatta Network Operating System

# Copyright Statement



The training materials and other content provided herein for assistance in training on the Vyatta vRouter may have references to Brocade as the Vyatta vRouter was formerly a Brocade product prior to AT&T's acquisition of Vyatta. Brocade remains a separate company and is not affiliated to AT&T.

# About This Guide

This addendum describes firewall functionality that was updated on the AT&T Vyatta vRouter (referred to as a virtual router, vRouter, or router in the guide) in release 1801.

# Zone-based firewall

This addendum describes the firewall local zone, which is a component of zone-based firewalls.

In a zone-based firewall, firewall rulesets are applied to traffic flowing between zones. There are two types of zones:

- Interface zones
- The Local zone

**Interface-based zones** are zones where one or more interfaces have been assigned as members.

**The local zone** is a single zone that has been assigned to represent traffic coming into or going out from the router itself. The local zone cannot contain any interfaces.

Firwall rulesets are assigned to traffic flowing in one direction between two zones. For example, firewall FW_A_TO_B is applied to traffic from ZONE_A to ZONE_B.

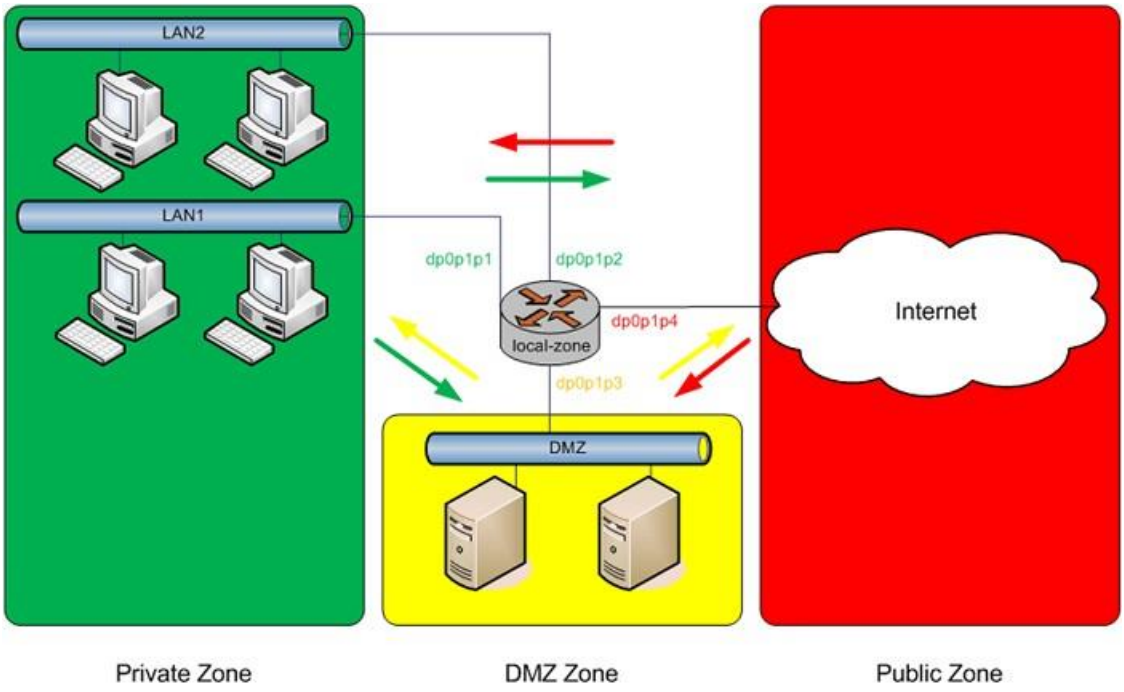
In a zone-based firewall, interfaces are grouped into security "zones," where each interface in a zone has the same security level.

Traffic flowing between interfaces includes within the same zone is not filtered; traffic flows freely because the interfaces share the same security level.

The following figure shows an example of a zone-based firewall implementation. This example has these characteristics:

- Three transit zones exist (that is, points where traffic transits the router): the private zone, the demilitarized zone (DMZ), and the public zone.
- The dp0p1p4 interface lies in the public zone; the dp0p1p1 and dp0p1p2 interfaces lie in the private zone; and the dp0p1p3 interface lies in the DMZ.
- The arrows from one zone to another zone represent traffic-filtering policies that are applied to traffic flowing between zones.
- Traffic flowing between LAN 1 and LAN 2 remains within a single security zone. Thus, traffic from LAN1 to LAN2, and traffic from LAN2 to LAN1 flows unfiltered.

Figure 2: Zone-based firewall overview




By default, all traffic coming into the router and originating from the router is allowed. Note the following additional points about zone-based firewalls:

- An interface can be associated with only one zone.
- An interface that belongs to a zone-based firewall cannot have interface-based firewall rule set applied to it, and conversely.
- Traffic between interfaces that do not belong to any zone flows unfiltered, and interface-based firewall rule sets can be applied to those interfaces.
- Traffic between interfaces that do not belong to any zone is not filtered by a zone-based firewall.
- Traffic between interfaces where only one interface is in a zone is always dropped.
- By default, all traffic to a zone is dropped unless explicitly allowed by a filtering policy for a source zone (**`from_zone`**) .
- Filtering policies are unidirectional; they are defined as a “zone pair” that identifies the zone from which traffic is sourced (**`from_zone`** ) and the zone to which traffic is destined (**`to_zone`** ). In the preceding figure, these unidirectional policies can be seen as follows:
- From private to DMZ
  - From public to DMZ
  - From private to public
  - From DMZ to public
  - From public to private
  - From DMZ to private

# Creating an Isolated Zone

You can create an isolated set of interfaces as follows:

- You can create a zone that has one or more interfaces and that does not have a loopback **lo** interface.
- Traffic between interfaces included within the zone is allowed.
- All traffic into and out of the zone is blocked.

For example, to create an isolated zone with three interfaces:

```
set security zone-policy zone ISOLATED interface dp0p1s0
set security zone-policy zone ISOLATED interface dp0p1s1
set security zone-policy zone ISOLATED interface dp0p1s2
```

## Control plane policing

Control plane policing (CPP) allows you to protect vRouter from excessive flooding by filtering control plane packet types. Control plane packets normally do not use much bandwidth. If the router is bombarded with unusually large amounts of control plane traffic, it is probably due to a denial-of-service (DoS) attack or a malfunction of a neighboring device.

CPP can be applied for interface-based firewalls and for zone-based firewalls. CPP for interface-based firewalls is described within the main body of the Firewall Configuration Guide.

This addendum describes CPP for zone-based firewalls.

# CPP for zone-based firewalls

If you are using zone-based firewalls, you can use the **local-zone** keyword to designate CPP as follows:

- You can designate *only one* zone as the local zone.
- You must specify rulesets for traffic from other zones to the local zone.
- (Optional) You can specify rulesets from traffic from the local zone to other zones.
- Traffic from the local zone is dropped only if an explicit block rule is matched.

### Additional points about control plane traffic coming into the router:

- If the ingress interface is not included in a zone, then control plane traffic is not filtered regardless of the presence or absence of the local zone.
- If the local zone is not specified , then control plane traffic is not filtered regardless of whether the ingress interface is included in a zone or not.
- If the ingress interface is included in a zone and a local zone is specified , then control plane traffic is dropped unless explicitly allowed by a ruleset.

### Additional points about control plane traffic originating from the router:

- If the local zone is not specified , then control plane traffic is not filtered regardless of whether the egress interface is included in a zone or not.

- If the local zone is specified and the egress interface is not included in a zone, then control plane traffic from the router is not filetered.
- If the egress interface is included in a zone and a local zone is specified , then control plane traffic is dropped unless explicitly allowed by a ruleset.

To configure a local zone, use the following commands::

| Purpose | Command |
|---|---|
| Designate one zone as the local zone | `set security zone-policy zone LOCAL local-zone` |
| Specify a ruleset for traffic from the PRIVATE zone to the local zone. | `set security zone-policy zone PRIVATE to LOCAL PRIV_TO_LOCAL` |
| Specify a ruleset for traffic from the PUBLIC zone to the local zones. | `set security zone-policy zone PUBLIC to LOCAL PUB_TO_LOCAL` |