EdgeRouter - Router on a Stick

help.ubnt.com/hc/en-us/articles/204959444

Overview

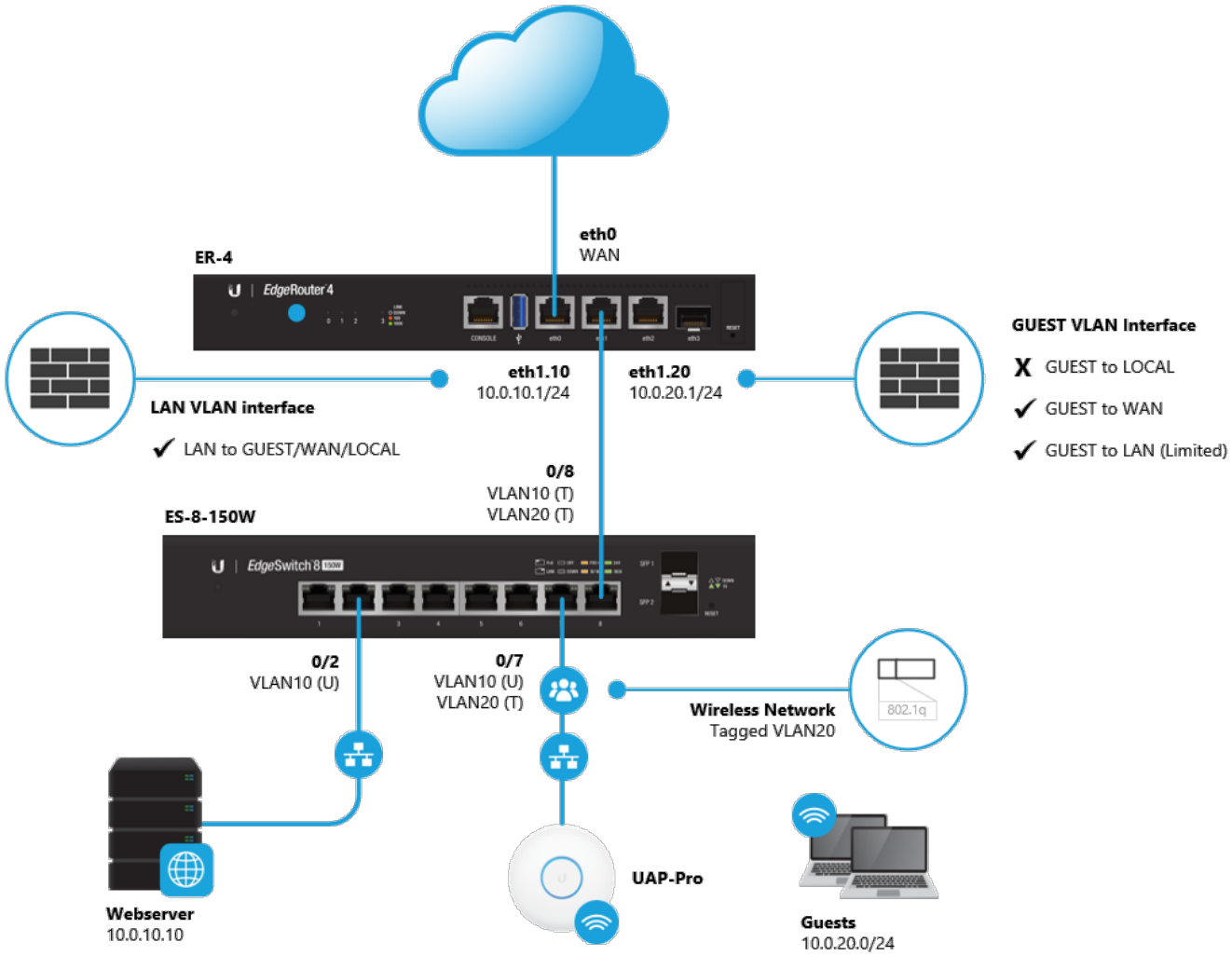
Readers will learn how to configure the EdgeRouter as a *Router on a Stick* using Virtual VLAN Interfaces (VIFs).

Applicable to the latest EdgeOS firmware on all EdgeRouter models. Please see the Related Articles below for more information.
Devices used in this article:

- EdgeRouter-4 (ER-4)
- ES-8-150W

How to Configure the Router on a Stick Setup

Back to Top



The EdgeRouter VLAN interfaces and firewall policies will be used to route and limit the traffic between VLAN10 and VLAN20.

The *Router on a Stick* setup allows the EdgeRouter to route traffic between VLANs by associating an Ethernet interface with multiple VLAN IDs. This allows the devices in different VLANs to communicate with each other through the EdgeRouter. The following VLANs are used in this example:

- `VLAN10` This is the 10.0.10.0/24 LAN network assigned to the eth1 VLAN10 interface (eth1.10).
- `VLAN20` This is the 10.0.20.0/24 GUEST network assigned to the eth1 VLAN20 interface (eth1.20).

Firewall rules are also added to limit the inter-VLAN traffic between VLAN10 and VLAN20. In this example, the guests in VLAN20 are only allowed to communicate with the Webserver in VLAN10. The following traffic is allowed:

- `GUEST to WAN` All traffic is allowed.

- `GUEST to LAN` Only HTTP and HTTPS requests to the Webserver at 10.0.10.10 is allowed.
- `GUEST to LOCAL` All traffic is dropped.

> **NOTE:** There is more information about EdgeRouter firewall states in the How to Create a WAN Firewall Rule article.

Follow the steps below to add the VLAN and firewall configuration to the EdgeRouter:

> **GUI:** Access the EdgeRouter Web UI.

1. Define the VLAN IDs and associate the interfaces with an IP address.

Dashboard > Add Interface > Add VLAN

VLAN ID: 10
Interface: eth1
Address: Manually define IP address
10.0.10.1/24

VLAN ID: 20
Interface: eth1
Address: Manually define IP address
10.0.20.1/24

2. Add DHCP scopes for the relevant VLANs.

Services > DHCP Server > Add DHCP Server

DHCP Name: vlan10
Subnet: 10.0.10.0/24
Range Start: 10.0.10.11
Range Stop: 10.0.10.150
Router: 10.0.10.1
DNS 1: 10.0.10.1

DHCP Name: vlan20
Subnet: 10.0.20.0/24
Range Start: 10.0.20.11
Range Stop: 10.0.20.150
Router: 10.0.20.1
DNS 1: 10.0.20.1

3. Enable DNS forwarding on the VLAN10 and VLAN20 interfaces.

Services > DNS > DNS Forwarding

Cache Size: 150
Interface: eth1.10
eth1.20

NOTE: There is more information about DNS Forwarding in the DNS Forwarding Setup & Options article.

4. Create the firewall rule that will prevent the guests in VLAN20 to manage the EdgeRouter.

Firewall/NAT > Firewall Policies > + Add Ruleset

Name: GUEST_LOCAL
Default action: Drop

5. Add a firewall rule to the newly created firewall policy that allows guests to use the EdgeRouter as a DNS server.

Firewall/NAT > Firewall Policies > GUEST_LOCAL > Actions > Edit Ruleset > + Add New Rule

Description: allow DNS
Action: Accept
Protocol: Both TCP and UDP
Destination > Port: 53

6. Add a firewall rule to the newly created firewall policy that allows guests to use the EdgeRouter as a DHCP server.

Firewall/NAT > Firewall Policies > GUEST_LOCAL > Actions > Edit Ruleset > + Add New Rule

Description: allow DHCP
Action: Accept
Protocol: UDP
Destination > Port: 67

7. Apply the firewall rule to the VLAN20 interface in the `local` direction.

Firewall/NAT > Firewall Policies > GUEST_LOCAL > Actions > Interfaces

Interface: eth1.20
Direction: local

8. Create the firewall rule that denies all traffic from VLAN20 to VLAN10, with the exception of HTTP and HTTPS requests to the Webserver.

Firewall/NAT > Firewall Policies > + Add Ruleset

Name: GUEST_IN
Default action: Accept

Firewall/NAT > Firewall Policies > GUEST_IN > Actions > Edit Ruleset > + Add New Rule

Description: webserver
Action: Accept
Protocol: TCP
Destination Address: 10.0.10.10
Destination Port: 80,443

Firewall/NAT > Firewall Policies > GUEST_IN > Actions > Edit Ruleset > + Add New Rule

Description: other
Action: Drop
Protocol: All protocols
Destination Address: 10.0.10.0/24

9. Apply the firewall rule to the VLAN20 interface in the `in` direction.

Firewall/NAT > Firewall Policies > GUEST_IN > Actions > Interfaces

Interface: eth1.20
Direction: in

The above configuration can also be set using the CLI:

> **CLI:** Access the Command Line Interface. You can do this using the CLI button in the GUI or by using a program such as PuTTY.

```
configure

set interfaces ethernet eth1 vif 10 address 10.0.10.1/24
set interfaces ethernet eth1 vif 20 address 10.0.20.1/24

set service dhcp-server shared-network-name vlan10 subnet 10.0.10.0/24 start 10.0.10.11 stop
10.0.10.150
set service dhcp-server shared-network-name vlan10 subnet 10.0.10.0/24 default-router 10.0.10.1
set service dhcp-server shared-network-name vlan10 subnet 10.0.10.0/24 dns-server 10.0.10.1

set service dhcp-server shared-network-name vlan20 subnet 10.0.20.0/24 start 10.0.20.11 stop
10.0.20.150
set service dhcp-server shared-network-name vlan20 subnet 10.0.20.0/24 default-router 10.0.20.1
set service dhcp-server shared-network-name vlan20 subnet 10.0.20.0/24 dns-server 10.0.20.1

set service dns forwarding cache-size 150
set service dns forwarding listen-on eth1.10
set service dns forwarding listen-on eth1.20

set firewall name GUEST_IN default-action accept

set firewall name GUEST_IN rule 10 action accept
set firewall name GUEST_IN rule 10 description webserver
set firewall name GUEST_IN rule 10 log disable
set firewall name GUEST_IN rule 10 protocol tcp
set firewall name GUEST_IN rule 10 destination port 80,443
set firewall name GUEST_IN rule 10 destination address 10.0.10.10

set firewall name GUEST_IN rule 20 action drop
set firewall name GUEST_IN rule 20 description other
set firewall name GUEST_IN rule 20 log disable
set firewall name GUEST_IN rule 20 protocol all
set firewall name GUEST_IN rule 10 destination address 10.0.10.0/24

set firewall name GUEST_LOCAL default-action drop

set firewall name GUEST_LOCAL rule 10 action accept
set firewall name GUEST_LOCAL rule 10 description 'allow dns'
set firewall name GUEST_LOCAL rule 10 log disable
set firewall name GUEST_LOCAL rule 10 protocol tcp_udp
set firewall name GUEST_LOCAL rule 10 destination port 53

set firewall name GUEST_LOCAL rule 20 action accept
set firewall name GUEST_LOCAL rule 20 description 'allow dhcp'
set firewall name GUEST_LOCAL rule 20 log disable
set firewall name GUEST_LOCAL rule 20 protocol udp
set firewall name GUEST_LOCAL rule 20 destination port 67

set interfaces ethernet eth1 vif 20 firewall in name GUEST_IN
set interfaces ethernet eth1 vif 20 firewall local name GUEST_LOCAL

commit ; save
```

Click to copy

Related Articles

Back to Top

Intro to Networking - How to Establish a Connection Using SSH

EdgeSwitch - Tagging and Untagging Port VLANs

EdgeRouter - Zone-Based Firewall

EdgeRouter - VLAN-Aware Switch

EdgeRouter - How to Create a Guest\LAN Firewall Rule