Securing Inter VLAN traffic

Deploying Palo Alto firewalls in layer 2 networks

PAN-OS 4.0– 4.1

Revision B

Contents

Overview

VLANs are used as an alternative solution to routers for broadcast containment. A Layer 2 switch can be configured to group subsets of ports into virtual broadcast domains isolated from each other. These domains are commonly known as virtual LANs (VLANs). Using a VLAN not only offers the benefit of containing traffic within a VLAN, but also provides security by restricting communication between hosts in different VLANs. A typical VLAN implementation will have hosts in each VLAN with a unique IP subnet. Inter VLAN communication, if required, is accomplished by routing the traffic between VLANs. In this tech note, we will discuss how Palo Alto Networks firewalls can be used to secure inter VLAN traffic when each VLAN has its own IP subnet and when a single IP subnet spans multiple VLANs.

Design requirement

Hardware requirement

Any Palo Alto Networks firewall.

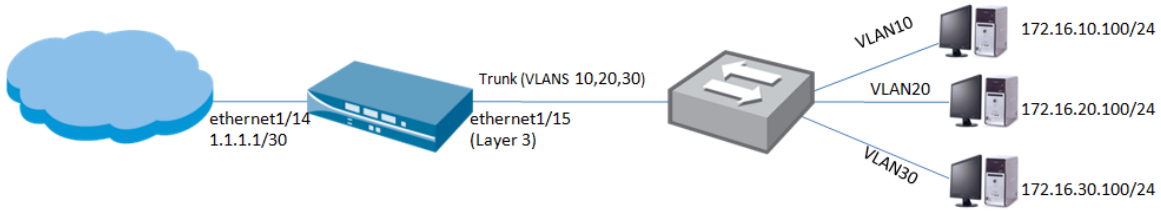
Software requirement

This document was tested with PAN-OS 4.0 and 4.1

Topology

Case1: Inter VLAN routing with each VLAN in a unique IP subnet

In order for network devices in different VLANs to communicate, a router must be used to route traffic between the VLANs. While VLANs help to control local traffic, if a device in one VLAN needs to communicate with a device in another VLAN, one or more routers must be used for inter VLAN communication. In this configuration a Palo Alto networks firewall can used to securely route traffic within the VLAN. This is also commonly called “one arm routing” or “router on a stick”.



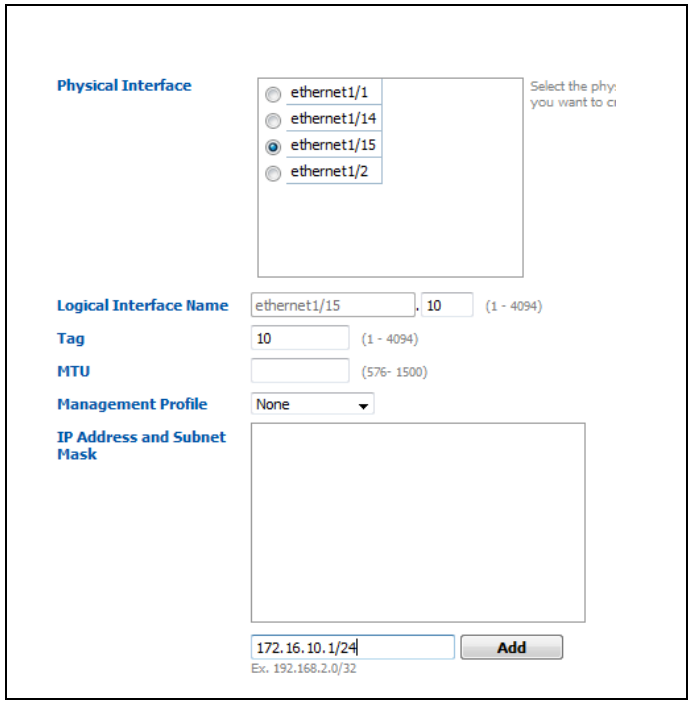
Configuration summary

The interface ethernet1/15 is configured as a layer 3 interface. Subinterfaces corresponding to each one of the VLAN are created off of the parent interface Ethernet 1/15. Each subinterface is assigned a VLAN tag and an IP address corresponding to the VLAN provides connectivity. Subinterfaces are assigned to separate zones to enforce security policy check on inter VLAN traffic. The table below summarizes the interface, zone, and VLAN configuration on the firewall.

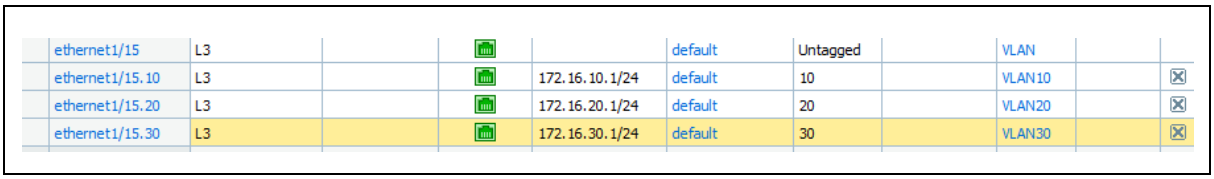
Interface	Interface type	Zone/Type	VR	IP address
Ethernet 1/15	Layer 3	Trust/layer3	default-vr	
Ethernet 1/15.10	Layer 3	VLAN10/layer3	default-vr	172.16.10.1/24
Ethernet 1/15.20	Layer 3	VLAN 20/layer3	default-vr	172.16.20.1/24
Ethernet 1/15.30	Layer 3	VLAN 30/layer3	default-vr	172.16.30.1/24

Interface configuration

Create a new Layer 3 interface, one for each VLAN. The following figure shows the screen shot for interface ethernet1/15.10 configured for VLAN 10. Note that the parent interface ethernet1/15 must be configured as a layer 3 interface.



With all the interfaces configured, the VLAN and interface configuration must look like the following screenshot:



Security policies

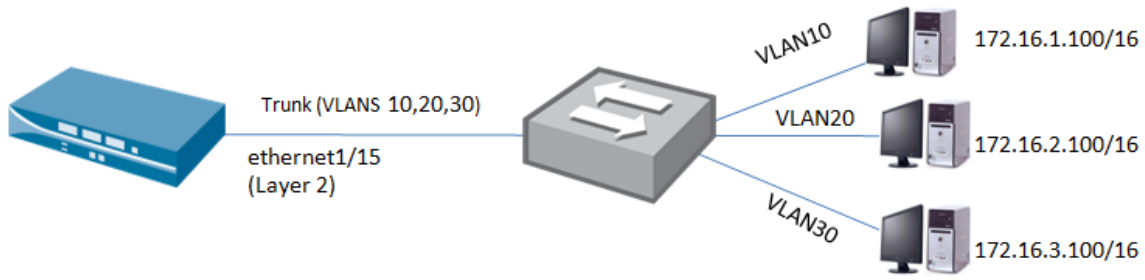
In this example, we allow oracle traffic from VLAN10 to VLAN20 as well as internet access for all VLANs.

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	rule1	VLAN10 VLAN20 VLAN30	untrust	any	any	any	any	any	✓	none	
2	rule2	VLAN10	VLAN20	any	any	any	oracle	any	✓	none	

Case 2: Single IP Subnet spanning multiple VLANs and rewriting VLAN tags

In this case, the same IP subnet spans multiple VLANs as shown in the following figure. The Palo Alto Networks firewall in configured in layer 2 mode and can be deployed to secure inter VLAN traffic.



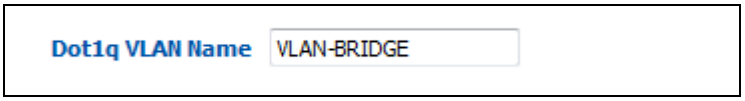
Configuration Summary

The interface ethernet1/15 is configured as a layer 2 interface. Subinterfaces corresponding to each one of the VLAN are created off of the parent interface ethernet1/15. These subinterfaces are then assigned to a single VLAN. The firewall treats each one of the VLAN logical interfaces as physical interfaces, all in the same VLAN. This allows the firewall to forward traffic between each of these interfaces since they are in the same VLAN, irrespective of the tag. In order to apply security policies, each of these individual interfaces can be assigned to its own zone. The table below summarizes the interface, zone, and VLAN configuration on the firewall.

Interface	Interface type	Tag	VLAN	Zone/Type
Ethernet 1/15	Layer 2	untagged	VLAN-BRIDGE	Trust-L2/layer2
Ethernet 1/15.10	Layer 2	10	VLAN- BRIDGE	VLAN10/layer2
Ethernet 1/15.20	Layer 2	20	VLAN-BRIDGE	VLAN 20/layer2
Ethernet 1/15.30	Layer 2	30	VLAN-BRIDGE	VLAN 30/layer2

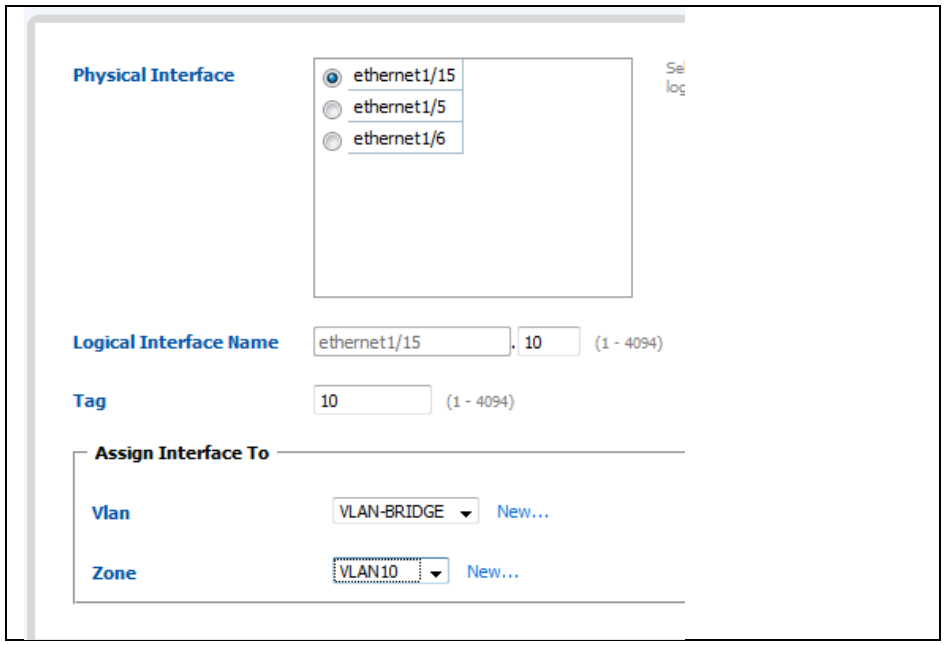
VLAN configuration

Create a new VLAN called Bridge_50to70. Navigate to network > vlans > new

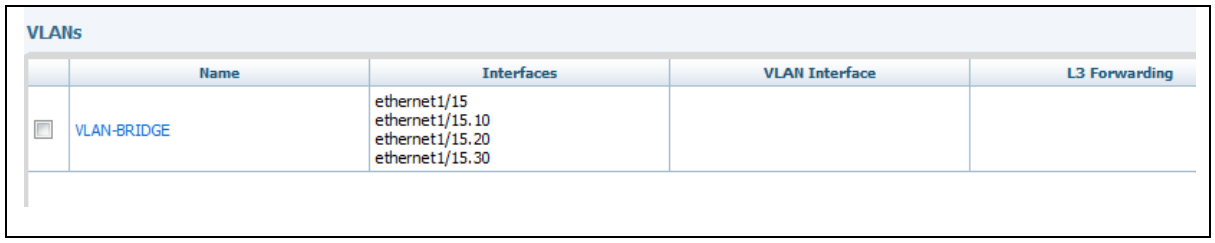


Interface Configuration

Create a new Layer 2 interface, one for each VLAN. Figure below shows the screen shot for interface ethernet1/15.10 configured for VLAN 10. Note that the parent interface ethernet1/15 must be configured as a layer 2 interface.



With the interfaces and VLAN configured, the interface configuration must look like the screenshot below



Security Policy

In this example we will permit only SSL traffic from VLAN10 to VLAN20.

Verification

Flow debug for SSL traffic initiated from the host 172.16.1.100 to 172.16.2.100 is shown below. For the sake of simplicity only the relevant sections of the flow debug is shown.

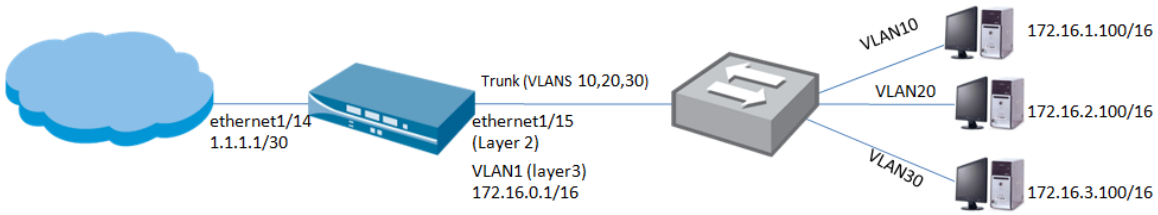
```
Packet received at slowpath stage
Packet info: len 70 port 30 interface 256
  wqe index 229357 packet 0x0x8000000416fb30e2
Packet decoded dump:
L2:     a4:ba:db:ba:3f:07->00:1b:17:00:01:1e, VLAN 10 (0x8100 0x000a),
type 0x0800
IP:     172.16.1.100->172.16.2.100, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 1119, frag_off 0x4000, ttl 128, checksum 39548
TCP:    sport 57032, dport 443, seq 3256824124, ack 0,
        reserved 0, offset 8, window 8192, checksum 8014,
        flags 0x0002 ( SYN), urgent data 0
TCP option:
00000000: 02 04 05 b4 01 03 03 02  01 01 04 02                .........
....
Session setup: vsys 1
Session setup: ingress interface ethernet1/15.10 egress interface
ethernet1/15.20 (zone 5)
Policy lookup, matched rule index 0
Allocated new session 52
Created session, enqueue to install

== Sep 10 11:53:29 ==
Packet received at fastpath stage
Packet info: len 70 port 30 interface 256
  wqe index 229357 packet 0x0x8000000416fb30e2
Packet decoded dump:
L2:     a4:ba:db:ba:3f:07->00:1b:17:00:01:1e, VLAN 10 (0x8100 0x000a),
type 0x0800
IP:     172.16.1.100->172.16.2.100, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 1119, frag_off 0x4000, ttl 128, checksum 39548
TCP:    sport 57032, dport 443, seq 3256824124, ack 0,
        reserved 0, offset 8, window 8192, checksum 8014,
        flags 0x0002 ( SYN), urgent data 0
TCP option:
00000000: 02 04 05 b4 01 03 03 02  01 01 04 02                .........
....
Flow fastpath, session 52
Forwarding lookup, ingress interface 256
L2 mode, VLAN 1
MAC entry found on VLAN 1, packet switched to interface ethernet1/15.20
L2 tag translation, replace VLAN tag with 20
Transmit packet on port 30

== Sep 10 11:53:29 ==
Packet received at np stage
Packet info: len 70 port 30 interface 257
  wqe index 229339 packet 0x0x8000000416ff70e2
Packet decoded dump:
L2:     00:1b:17:00:01:1e->a4:ba:db:ba:3f:07, VLAN 20 (0x8100 0x0014),
type 0x0800
IP:     172.16.2.100->172.16.1.100, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 0, frag_off 0x4000, ttl 64, checksum 57051
TCP:    sport 443, dport 57032, seq 1526252708, ack 3256824125,
```

```
        reserved 0, offset 8, window 5840, checksum 2252,
        flags 0x0012 ( SYN ACK), urgent data 0
TCP option:
00000000: 02 04 05 b4 01 01 04 02  01 03 03 06                ........
....

== Sep 10 11:53:29 ==
Packet received at np stage
Packet info: len 64 port 30 interface 256
  wqe index 229295 packet 0x0x8000000416fec8e2
Packet decoded dump:
L2:     a4:ba:db:ba:3f:07->00:1b:17:00:01:1e, VLAN 10 (0x8100 0x000a),
type 0x0800
IP:     172.16.1.100->172.16.2.100, protocol 6
        version 4, ihl 5, tos 0x00, len 40,
        id 1120, frag_off 0x4000, ttl 128, checksum 39559
TCP:    sport 57032, dport 443, seq 3256824125, ack 1526252709,
        reserved 0, offset 5, window 16425, checksum 8260,
        flags 0x0010 ( ACK), urgent data 0
TCP option:

== Sep 10 11:53:29 ==
Packet received at fastpath stage
Packet info: len 70 port 30 interface 257
  wqe index 229339 packet 0x0x8000000416ff70e2
Packet decoded dump:
L2:     00:1b:17:00:01:1e->a4:ba:db:ba:3f:07, VLAN 20 (0x8100 0x0014),
type 0x0800
IP:     172.16.2.100->172.16.1.100, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 0, frag_off 0x4000, ttl 64, checksum 57051
TCP:    sport 443, dport 57032, seq 1526252708, ack 3256824125,
        reserved 0, offset 8, window 5840, checksum 2252,
        flags 0x0012 ( SYN ACK), urgent data 0
TCP option:
00000000: 02 04 05 b4 01 01 04 02  01 03 03 06                ........
....
Flow fastpath, session 52
Forwarding lookup, ingress interface 257
L2 mode, VLAN 1
MAC entry found on VLAN 1, packet switched to interface ethernet1/15.10
L2 tag translation, replace VLAN tag with 10
Transmit packet on port 30
```

Traffic Log

Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action	Rule	Ingress I/F	Egress I/F	Bytes
09/10 13:51:45	end	VLAN10	VLAN20	172.16.1.100	172.16.2.100	57929	443	tcp	ssl	allow	rule1	ethernet1/15.10	ethernet1/15.20	81465
09/10 13:51:45	end	VLAN10	VLAN20	172.16.1.100	172.16.2.100	57928	443	tcp	ssl	allow	rule1	ethernet1/15.10	ethernet1/15.20	34175
09/10 13:51:45	end	VLAN10	VLAN20	172.16.1.100	172.16.2.100	57931	443	tcp	ssl	allow	rule1	ethernet1/15.10	ethernet1/15.20	23031

Case 2a: Extending connectivity beyond 172.16.0.0/16 subnet

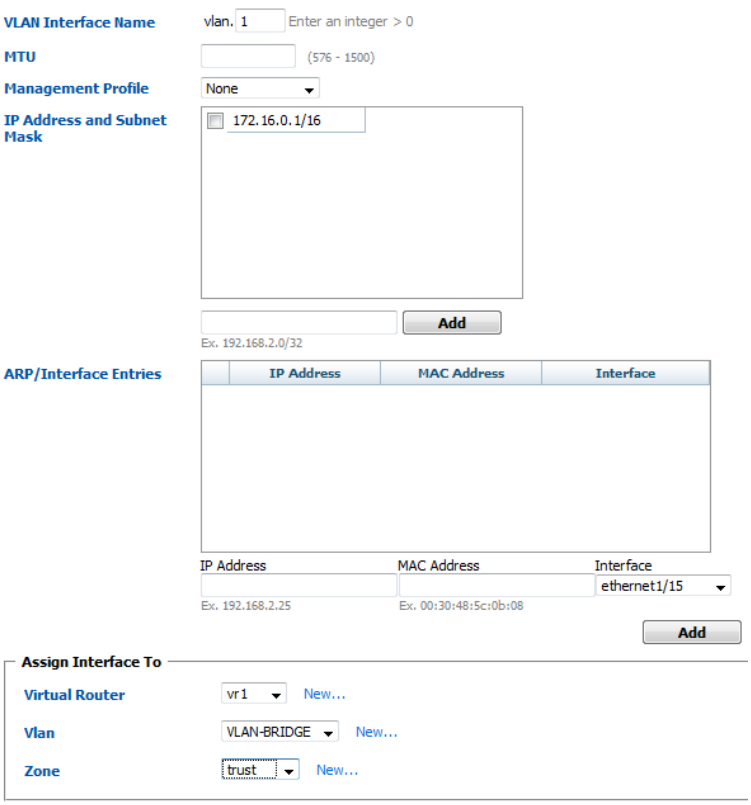


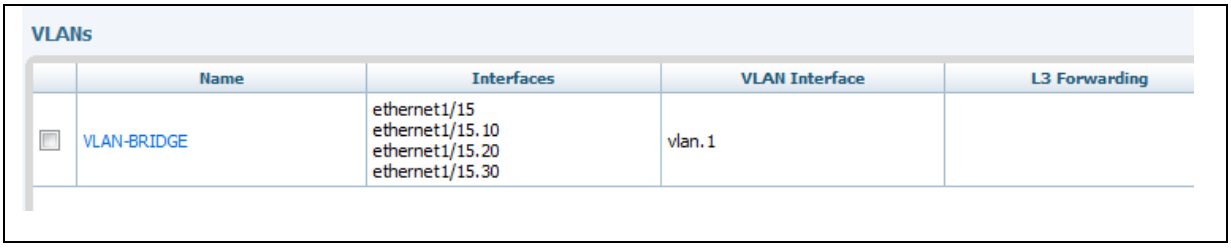
The configuration discussed in Case2 can be extended to provide connectivity beyond the network 172.16.0.0/16. This is done by creating a logical VLAN interface to route traffic in and out of the VLAN. The hosts in all VLANs are configured to have the default gateway pointing to the VLAN1 interface 172.16.0.1/16. Any traffic to destination other than 172.16.0.0/16 will be sent to the VLAN1 interface to be routed.

The following table summarizes the interface configuration:

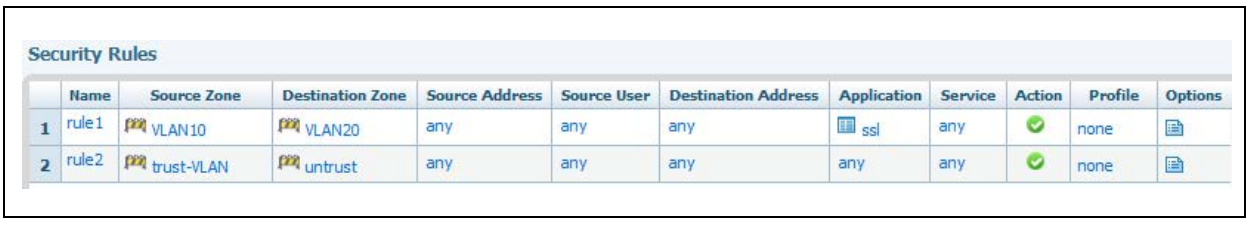
Interface	Interface type	Tag	VLAN	Zone/Type
Ethernet 1/15	Layer 2	untagged	VLAN-BRIDGE	Trust-L2/layer2
Ethernet 1/15.10	Layer 2	10	VLAN- BRIDGE	VLAN10/layer2
Ethernet 1/15.20	Layer 2	20	VLAN-BRIDGE	VLAN 20/layer2
Ethernet 1/15.30	Layer 2	30	VLAN-BRIDGE	VLAN 30/layer2
VLAN.1	Layer 3	untagged	VLAN-BRIDGE	trust/layer3

The following figure shows the screenshot of the VLAN1 interface configuration.





All traffic for destination other than 172.16.0.0/16 will be forwarded to the VLAN.1 interface. It is important to understand the security policies must be created between the layer3 zones, i.e. trust-VLAN zone where the VLAN.1 interface is untrust zone, and where the ethernet1/14 interface is bound. The following figure shows the security rules required to permit access from VLAN10 and VLAN20 to the external network.



NAT can also be applied to traffic from the VLANs. Sample NAT configuration to translate all traffic from trust-VLAN to the egress interface IP is shown in the following table:

NAT Rules

		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	trust	untrust	any	any	any	any	dynamic-ip-and-port , ethernet1/14 , 1.1.1.1/30	none

Summary

Palo Alto Networks firewalls provide a very flexible architecture to deploy and secure layer2 networks, while still offering the benefits of App-ID, Content-ID, and User-ID.

Revision History

Date	Revision	Comment
May 15, 2012	B	Updated for PAN-OS 4.0 and 4.1