Queensland Audi/VW Network

2010-10-04
Michael Spence

Audience:

Currently this documentation is for Network Administrators only. In the future, I do not foresee as yet other appropriate persons to whom this document may apply. It is assumed that the Network Administrator has an understanding of Firewalling and Routing techniques.

Preamble:

This document describes the required network setup for the Audi & VW connections. This document details the required routes and methodology used to create these routes on the Qld Firewall, demonstrating how a client can gain connectivity to the Audi/VW Extranets.

Clients:

All clients are considered to be computers within the Qld APEagers Network, most notably the Austral Audi users (at Currimundi) and the Austral VW users (at Newstead). For reference, these computers exist on the internal networks of 10.35.0.0/16 and 10.10.0.0/16 respectively.

Audi/VW supplied Equipment:

The connections to Audi and VW are made available using the Audi/VW supplied Juniper. This device creates a VPN between both Audi and VW. This device is the property of Audi/VW.

Some Audi/VW programs/tools talk directly to servers within our network. For this purpose Audi/VW originally supplied a server, which has since been virtualised. This computer has the name "au220400s01001" but will be referenced as the BTAC server hereafter.

Audi/VW Subnets and Hosts:

As supplied by Audi and VW the following lists are destination networks and hosts, to which clients connect.

Audi:	VW:
10.112.192.0/24	10.112.198.0/24
10.166.145.0/24	10.112.230.0/24
	10.152.15.0/24
	172.16.61.0/24
	210.193.223.156

Juniper Setup:

The Juniper has two types of interfaces; trusted interfaces and an untrusted interface. Naturally the trusted interfaces exist on the internal network and the untrusted interface faces the internet. One trusted interface, which exists on the Internal Vlan, has been configured with the IP address of 10.1.1.240. The external interface, which exists on the B2B Vlan within the data centre, has the IP address of 10.40.1.61.

The firewall routes traffic, destined for the networks and hosts listed above, from the clients to the internal interface of the Juniper. The Juniper routes and alters this traffic using its proprietary VPN method. All traffic from the Juniper is routed to the Internet.

All traffic originating from the Audi and VW Junipers (the Junipers on the Audi and VW networks) from the internet, is specifically allowed to pass through the firewall and is redirected to our Juniper. This traffic is routed and altered according to the VPN method to clients or BTAC servers.

Traffic Flow:

The following is a step by step demonstration of how a typical client sends data to the Audi/VW networks.

1. Client initiates access to a Audi/VW network/host
2. Client's default route is to their local gateway into the WAN
3. WAN directs traffic to the Data Centre
4. Data Centre's default route is to the Firewall
5. Firewall determines access to Audi/VW network/host
6. Firewall routes traffic to internal interface of Juniper
7. Juniper initiates traffic destined for the internet
8. Firewall passes traffic to the internet

The following is a step by step demonstration of how typical data is sent from Audi/VW to internal devices.

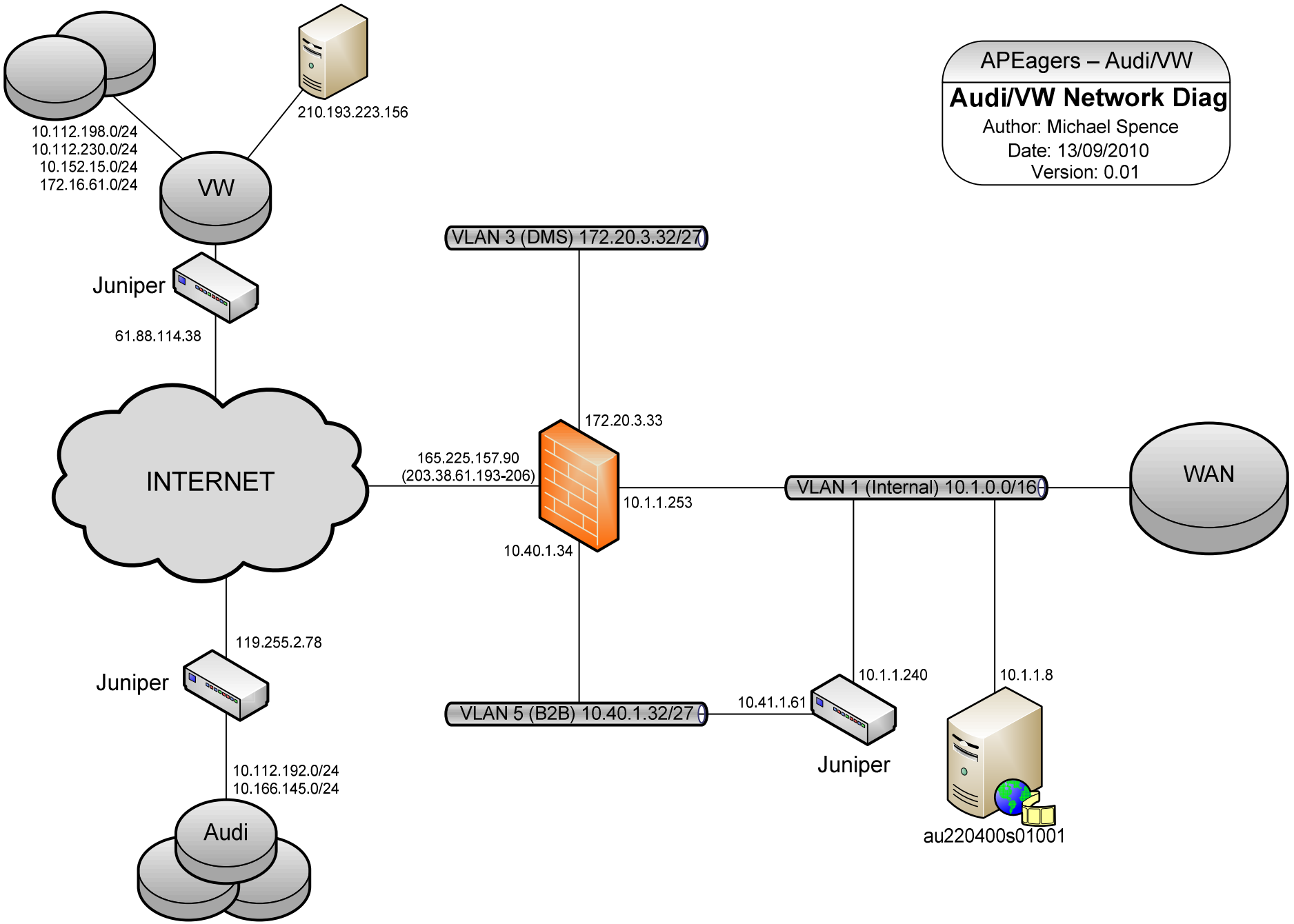
1. Audi/VW initiates access to an APEagers Client/Device (Unknown Network)
2. Audi/VW Juniper routes traffic to our External IP address (Internet Address)
3. All traffic from the internet passes through the Firewall
4. Firewall determines traffic from External Audi/VW Juniper
5. Firewall routes traffic to Internal Audi/VW Juniper
6. Juniper routes traffic to internal destination
   *** NOTE Firewall does not process this outbound traffic ***
7. If destination is in the WAN traffic is routed to specific Subnet

Applicable Firewall Rules:

```
# MACROS
int_vga_juniper =       "10.1.1.240"
b2b_vga_juniper =       "10.40.1.61"
sites_audi =            "10.112.192.0/24, 10.112.230.0/24, 10.166.145.0/24,
61.88.114.35"
sites_vw =              "10.112.198.0/24, 10.152.15.0/24, 172.16.61.0/24,
210.193.223.156"

# TABLES
table <proxy_bypass> const { $sites_audi, $sites_vw, .. et al }
table <inet_vwaudi> const { 59.154.32.6, 61.88.114.38, 119.225.2.78, 210.48.210.1
}
table <xnet_audi> const { 10.112.192.0/24, 10.166.145.0/24 }
table <xnet_vw> const { 10.112.198.0/24, 10.112.230.0/24, 10.152.15.0/24, \
       172.16.61.0/24, 210.193.223.156 }

# NATS
nat on $int_if from any to <xnet_audi> -> $int_if
nat on $int_if from any to <xnet_vw> -> $int_if

# RDRS
rdr on $ext_if from <inet_vwaudi> to any -> $b2b_vga_juniper

# FILTERS
pass in log quick on $ext_if from <inet_vwaudi> to $b2b_vga_juniper keep state
pass in quick on $int_if proto { tcp, udp } from \
       any to <proxy_bypass> port { $inet_ports }
pass quick on $b2b_if no state
```

Applicable Firewall Routes:

```
# Audi Routes
route -n add -net 10.112.192.0/24 10.1.1.240
route -n add -net 10.166.145.0/24 10.1.1.240

# VW Routes
route -n add -net 10.112.198.0/24 10.1.1.240
route -n add -net 10.112.230.0/24 10.1.1.240
route -n add -host 10.112.230.8 10.1.1.240
route -n add -net 10.152.15.0/24 10.1.1.240
route -n add -net 172.16.61.0/24 10.1.1.240
route -n add -host 210.193.223.156 10.1.1.240
```


APEagers – Audi/VW
Audi/VW Network Diag
Author: Michael Spence
Date: 13/09/2010
Version: 0.01
10.112.198.0/24
10.112.230.0/24
10.152.15.0/24
172.16.61.0/24
210.193.223.156
VW
Juniper
61.88.114.38
INTERNET
119.255.2.78
Juniper
10.112.192.0/24
10.166.145.0/24
Audi
VLAN 3 (DMS) 172.20.3.32/27
172.20.3.33
165.225.157.90
(203.38.61.193-206)
10.1.1.253
10.40.1.34
VLAN 1 (Internal) 10.1.0.0/16
WAN
VLAN 5 (B2B) 10.40.1.32/27
10.41.1.61
Juniper
10.1.1.240
10.1.1.8
au220400s01001