Qld & NT Audi Network

2010-11-15
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 connections at Audi Centre Sunshine Coast and Audi Centre Darwin. 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 Extranets and BTAC server.

Clients:

All clients are considered to be computers within the Qld APEagers Network, most notably the Audi users at Currimundi and at Berrimah. For reference, these computers exist on the internal networks of 10.35.0.0/16 and 10.52.0.0/16 respectively.

Audi supplied Equipment:

The connections to Audi 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. (It is believed that the Juniper currently being used is the original. Audi Australia have supplied a second Juniper, but as the current setup is working effectively it has never been installed.)

The service centres at Sunshine Coast and Darwin, each have an Audi supplied diagnostics machine, otherwise known as a VAS machine. The details for each machine are:

Sunshine Coast:
Name: au457700o00010
MAC: 0030-d602-5538
IP: 10.35.1.111
Model: 5051b

Name: vas5052a
MAC: 0030-d603-c7b2
IP: 10.35.1.112
Model: 5052a

Darwin:
Name: au082800o00010
MAC: 0030-d601-c5b2
IP: 10.52.1.191
Model: 5051b

At each of their respective local sites there is a DHCP server, with reservations for these MAC addresses. These reservations supply alternate configurations to the other computers on the network.

Some Audi programs/tools talk directly to servers within our network. For this purpose Audi originally supplied a server, which has since been virtualised. This computer has the name "au457700s00001" but will be referenced as the BTAC server hereafter. The Audi BTAC server has an IP address of 10.1.1.16. The administrator password is “tamwood”.

Audi Subnets and Hosts:

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

Audi:
10.112.192.0/24
10.166.145.0/24

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 Junipers (the Junipers on the Audi 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 network.

1. Client initiates access to a Audi 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 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 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 Juniper
5. Firewall routes traffic to Internal Audi 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"

# TABLES
table <proxy_bypass> const { $sites_audi, .. 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 }

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

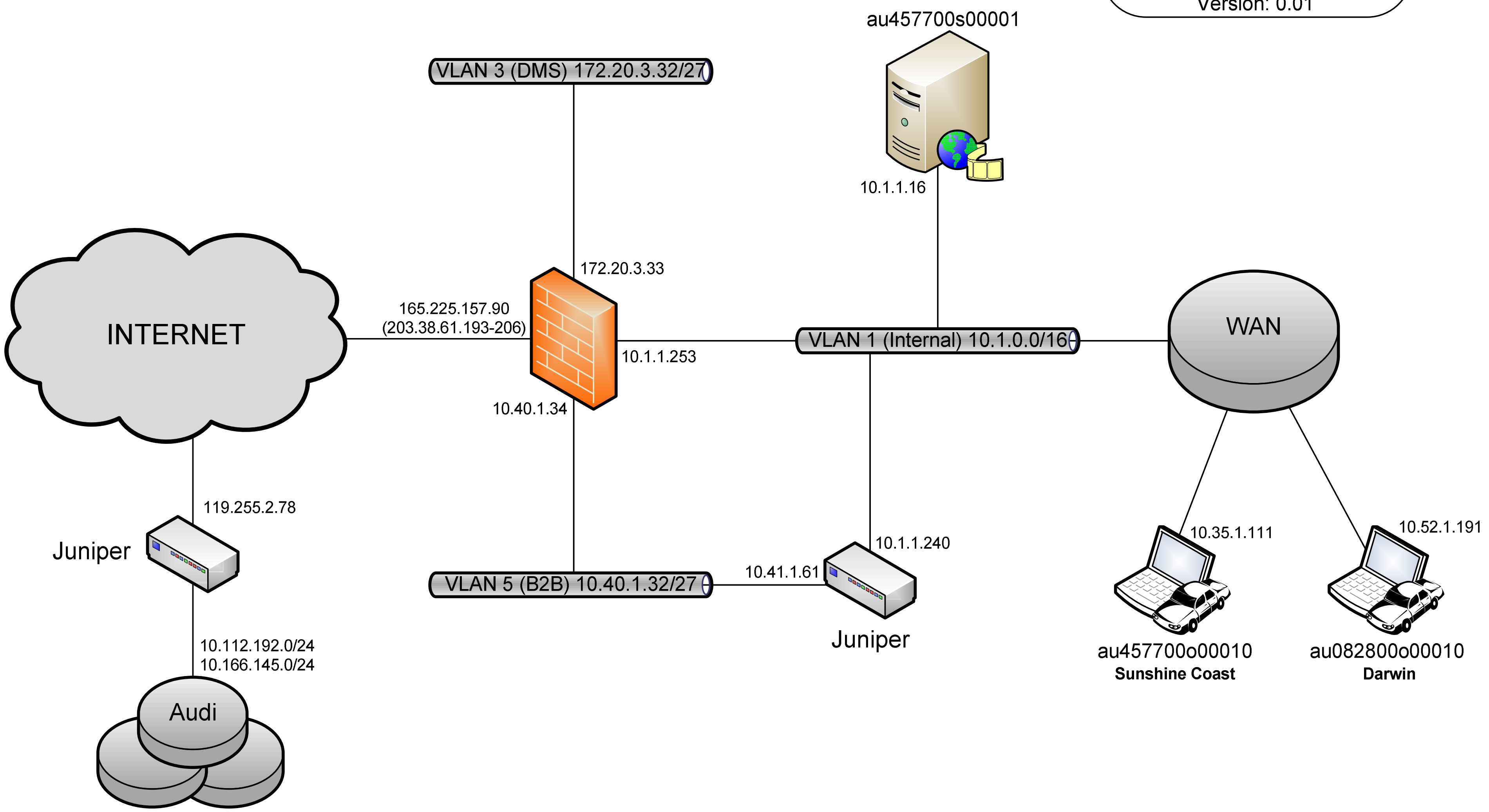
Applicable Firewall Routes:

```
# 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
```

APEagers – Audi Qld/NT

Audi Network Diag

Author: Michael Spence
Date: 15/11/2010
Version: 0.01


au457700s00001
10.1.1.16
VLAN 3 (DMS) 172.20.3.32/27
172.20.3.33
INTERNET
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
119.255.2.78
Juniper
10.112.192.0/24
10.166.145.0/24
Audi
VLAN 5 (B2B) 10.40.1.32/27
10.41.1.61
10.1.1.240
Juniper
10.35.1.111
au457700o00010
Sunshine Coast
10.52.1.191
au082800o00010
Darwin