Klosters BMW 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 BMW connections. This document details the required routes and methodology used to create these routes on the Klosters Firewall, demonstrating how a client can gain connectivity to the BMW Extranets and BMW can gain access to the ICOM devices.

Clients:

All clients are considered to be computers within the Klosters APEagers Network, most notably the Klosters BMW users (at Newcastle). For reference, these computers exist on the internal network of 172.17.104.0/22.

BMW supplied Equipment:

There are a number of devices supplied/configured by BMW inside our network. These include two (2) ISIS servers and a number of ICOM devices (only one of which is contactable by BMW). ISIS servers are media servers which contain up to date specification sheets and diagnosis utilities. The ICOMs are the diagnosis devices, which attach to cars and communicate directly with the cars' onboard computers.

The ICOM devices talk directly to the ISIS servers (this is my belief – not verified with BMW) for up to date servicing details. The ISIS computers request updates from BMW (generally from Germany – again my belief). BMW Australia talks to one ICOM, for which the firewall has been configured.

BMW Subnets and Hosts:

As supplied by BMW the following lists are destination networks and hosts, to which clients connect. *** This list is inaccurate and misleading. What is required is a list of the destinations to which the ISIS servers connect. ***

BMW:
203.44.204.4

Firewall Setup:

Currently the firewall is not fully configured, but at this time does provide all the functionality required for BMW. At present the firewall does not block any internally generated internet traffic, which (I believe) allows the ISIS servers to contact Germany or alternate BMW locations on the web.

For BMW Australia to contact the ICOM device, Special firewall rules have bee put in place to redirect traffic from BMW Australia to the one ICOM device setup for this purpose.

Applicable Firewall Rules:

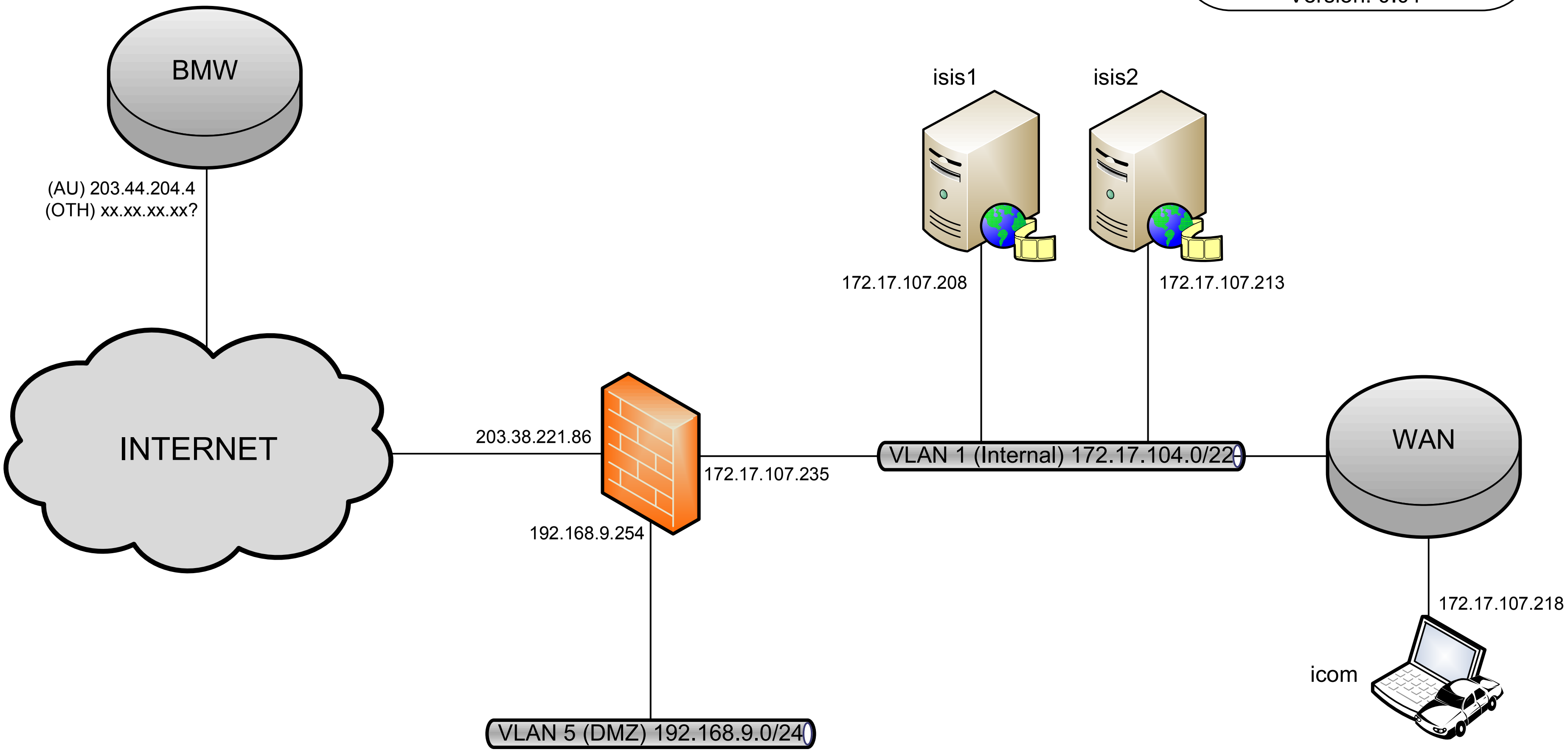
```
# MACROS
inet_bmw_aust =            "203.44.204.4"
int_bmw_icom =             "172.17.107.218"

# TRANSLATION
rdr on $ext_if proto tcp from $inet_bmw_aust \
       to any port { $bmw_ports } -> $int_bmw_icom

# FILTERING
pass out all
pass in log quick on $ext_if proto tcp from $inet_bmw_aust \
       to $int_bmw_icom port { $bmw_ports }
```

***** NOTE: Firewall should be altered to only allow specific servers access to internet *****

APEagers - KLB

Klosters BMW Network

Author: Michael Spence
Date: 7/10/2010
Version: 0.01


BMW
(AU) 203.44.204.4
(OTH) xx.xx.xx.xx?
INTERNET
203.38.221.86
172.17.107.235
192.168.9.254
VLAN 5 (DMZ) 192.168.9.0/24
isis1
isis2
172.17.107.208
172.17.107.213
VLAN 1 (Internal) 172.17.104.0/22
WAN
172.17.107.218
icom