Comware packet-filters applied to a VLAN interface now impact local traffic on the VLAN

SUPPORT COMMUNICATION - CUSTOMER BULLETIN

Document ID: c04335560
Version: 1

```
Comware packet-filters applied to a VLAN interface now impact local
traffic on the VLAN
```

NOTICE: The information in this document, including products and software versions, is current as of the Release Date. This document is subject to change without notice.

Release Date: 2014-06-09
Last Updated: 2014-08-01

DESCRIPTION

A change has been introduced in recent software that changes the way ACLs are implemented when they are applied to VLAN interfaces.

Prior to the software change, a packet-filter ACL applied to a VLAN interface would only impact traffic traversing the VLAN interface between the VLAN and other VLANs/networks. Following the software change, an ACL applied to a VLAN interface also filters the local data on the VLAN itself.

In particular, it is possible that all local traffic on a VLAN may be blocked after upgrading to software that implements this change. For example, if a customer implements an ACL with a default "deny ip" rule intended to block undesirable access between networks, it will now also block traffic within the same VLAN:

```
# Define ACL
acl number 3600 name test-acl-in
hardware-count enable
rule 10 permit ip destination 172.22.254.0 0.0.0.255
rule 20 deny ip

#Apply ACL to Vlan interface
interface Vlan-interface600
ip address 10.90.32.1 255.255.255.0
packet-filter name test-acl-in inbound
```

Previously this ACL would have permitted all traffic on the VLAN, but blocked all non-permitted IP traffic traversing to other VLANs. After the software upgrade, the same rule blocks all IP traffic within the VLAN.

SCOPE

This change impacts a large number of products as defined below.

Product Name	Software versions with the change
5800/5820 Switches	R1808P16 and later
5500HI Switches	R5206P02 and later
5500EI/5500SI/5120EI Switches	R2220P11 and later
3600 EI and SI V2 Switches	R2108P10 and later
5900/5920 Switches	R2307 and later
5830 Switches	R1118P05
10500 Switches	R1208P06 and later
7500 Switches	R6708P06 and later
11900 (V7) Switches	R2105P05 and later
10500 (V7) Switches	R2105P05 and later
12900 (V7) Switches	R1005P01 and later

RESOLUTION

PRIOR to updating to the affected software versions, modify ACL definitions with rules to specifically permit the required intra-VLAN traffic.

Using the example above, the ACL will be modified to permit some local IP traffic using an additional rule (15) in the ACL definition as follows:

```
acl number 3600 name test-acl-in


hardware-count enable

rule 10 permit ip destination 172.22.254.0 0.0.0.255
rule 15 permit ip source 10.90.32.11 24 destination 10.90.32.12 24
rule 20 deny ip
```

This ACL will now allow communication within the VLAN.

HP regrets any inconvenience associated with this change.

Hardware Platforms Affected: HP 10500 Switch Series, HP 3600 EI Switch Series, HP 3600 SI Switch Series, HP 5120 EI Switch Series, HP 5500 EI Switch Series, HP 5500 HI Switch Series, HP 5500 SI Switch Series, HP 5800 Switch Series, HP 5820 Switch Series, HP 5830 Switch Series, HP 5900 Switch Series, HP 5920 Switch Series, HP 7500 Switch Series, HP FlexFabric 11900 Switch Series, HP FlexFabric 12900 Switch Series
Components Affected: Not Applicable
Operating Systems Affected: Not Applicable

Software Affected: Not Applicable
Third Party Products Affected: Not Applicable
Support Communication Cross Reference ID: IA04335560

REVISION HISTORY
1