Technical Support Note

TCP Window Scaling in Windows through the AOS Firewall

Introduction

PCs running Microsoft Windows Vista or Windows 7 may experience unexpected latency when communicating to other PCs in a different subnet through an AOS router running the firewall. Microsoft has enabled TCP Window Scaling in Windows Vista and Windows 7 which was not previously enabled by default in other Windows operating systems. TCP Window Scaling allows the PC to advertise a TCP receive window larger than 65,535 via a new TCP option called "Window Scale" to increase throughput of TCP sessions.

Symptoms

The AOS firewall has a hard coded maximum of 65,535 for TCP window size. Any packet beyond that maximum size will get dropped and trigger the following firewall message:

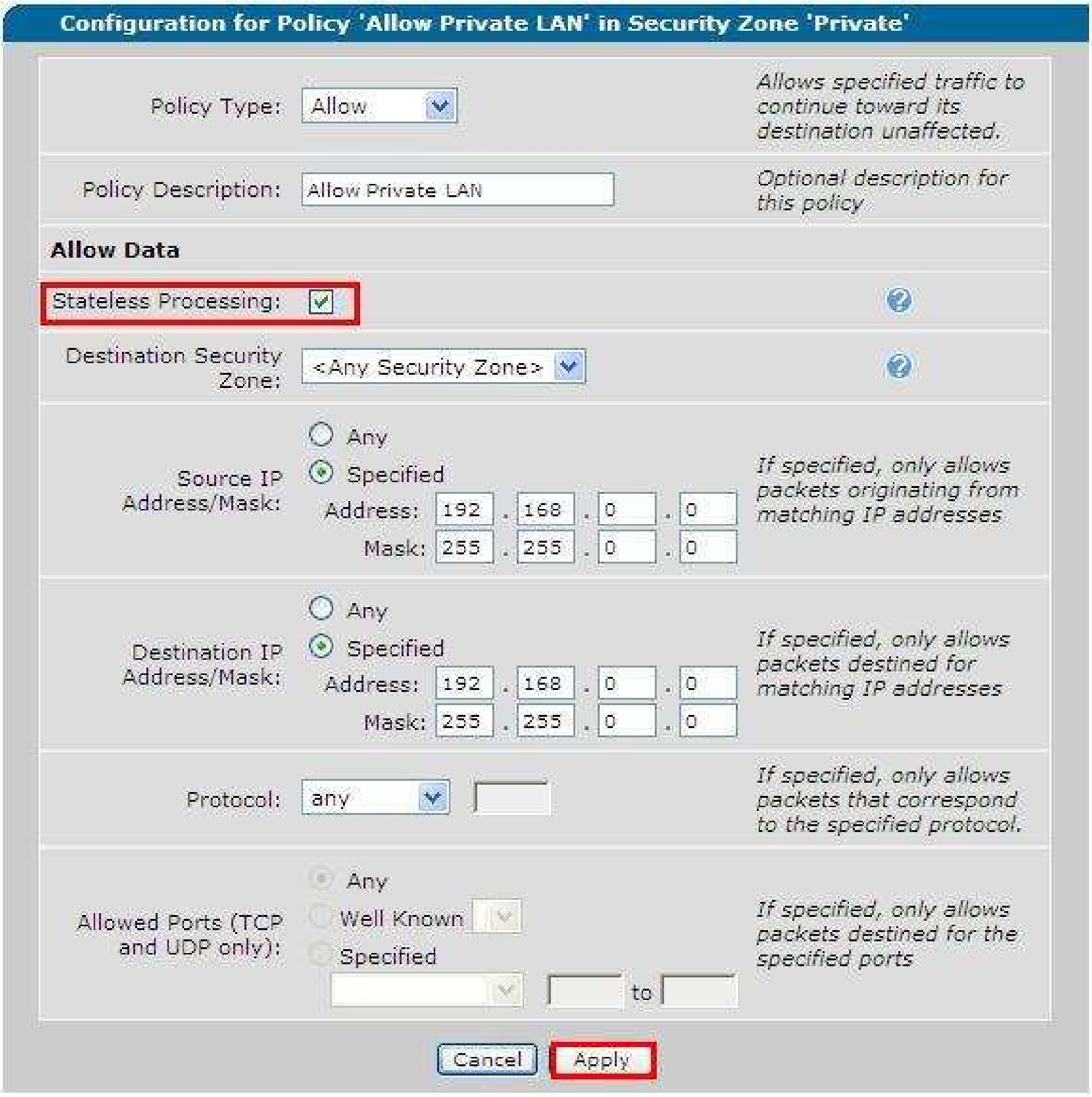
```
"Dropping pkt; sequence number out-of-range, seq=xxxx, high=yyyy"
```

This message will be seen in the event history of the AOS router, but the frequency of its visibility is dependant on the value specified with the **ip firewall policy-log threshold** command in the unit's current configuration.

Solution

Since the AOS firewall does not support the increased TCP window, one of two actions must be taken.

First, in the case of LAN to LAN traffic, the traffic in question should be allowed in a stateless firewall policy. To enable stateless processing in the GUI, navigate to Data > Security Zones > Private > and click the appropriate allow rule for the LAN to LAN traffic. On the resulting screen enable Stateless Processing by selecting the appropriate check box and clicking the Apply button.



Configuration for Policy 'Allow Private LAN' in Security Zone 'Private'

Policy Type: Allow — *Allows specified traffic to continue toward its destination unaffected.*

Policy Description: Allow Private LAN — *Optional description for this policy*

Allow Data

Stateless Processing: ☑

Destination Security Zone: <Any Security Zone>

Source IP Address/Mask: ○ Any ● Specified
Address: 192 . 168 . 0 . 0
Mask: 255 . 255 . 0 . 0
If specified, only allows packets originating from matching IP addresses

Destination IP Address/Mask: ○ Any ● Specified
Address: 192 . 168 . 0 . 0
Mask: 255 . 255 . 0 . 0
If specified, only allows packets destined for matching IP addresses

Protocol: any — *If specified, only allows packets that correspond to the specified protocol.*

Allowed Ports (TCP and UDP only): ● Any ○ Well Known ○ Specified ___ to ___
If specified, only allows packets destined for the specified ports

Second, TCP windowing can be disabled within the Windows operating system. Instructions for doing so can be found in the following Microsoft article: http://support.microsoft.com/kb/934430