ASA VPN Load Balancing Master Election Process

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Load-Balancing Algorithm
Master Election Process
Caveat for Reboot Scenarios
Master Reelection Process
Master Device Removed from the Cluster
Master Device does Not Respond to Cluster Member Hello Messages
Troubleshoot
Related Information

Introduction

This document describes the Master Election process in a VPN load-balancing scenario with the Cisco 5500-X Series Adaptive Security Appliance (ASA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco ASA 5500-X that runs software Version 9.2.

Note: This document also applies to all software versions, since the feature was first introduced in Version 7.0(1).
Background Information

VPN load balancing is a mechanism that is used in order to equitably distribute network traffic among the devices in a virtual cluster. Load balancing is based on simple distribution; it does not take in to account throughput utilization or other factors. A load-balancing cluster consists of two or more devices, a master and one or more secondary devices, and these devices do not have to be configured identically.

Load-Balancing Algorithm

Here is an overview of the load-balancing algorithm:

- The master device maintains a sorted list of secondary cluster members in ascending order of inside IP addresses.

- The load is computed as an integer percentage (number of active/maximum sessions) that is supplied by each secondary cluster member.

- The master device redirects the IPSec/Secure Sockets Layer (SSL) VPN tunnel to a device with the lowest load first, until it is one percent higher than the other devices.

- The master device redirects to itself only when all of the secondary cluster members are one percent higher than the master device.

Here is an example with one master and two secondary cluster members:

- All nodes begin with a zero-percent load, and all percentages are rounded to the nearest half-percent.

- The master device takes the connection if all of the members have a load that is one percent higher than the master device.

- If the master device does not take the connection, the session is taken by the backup device that currently has the smallest load percentage.

- If all of the members have the same load percentage, then the backup device with the least amount of sessions takes the session.

- If all of the members have the same load percentage and the same number of sessions, then the backup device with the least amount of IP addresses takes the session.

Master Election Process
The VPN load balancing Master Election process is performed on the cluster outside network. There are two types of data exchanged on the outside network:

- Address Resolution Protocol (ARP) packets for the cluster IP address that are used for master discovery are exchanged. The maximum number of ARP packets that are sent for the cluster IP address in order to discover the master is:

\[(10 - \text{priority}) + 1\]

Here, priority is configured as in the priority subcommand of the \texttt{vpn load-balancing} CLI command.

- UDP packets on the outside for the Hello request/response messages are exchanged. The port number is specified in the \texttt{cluster port} load-balancing subcommand and is default to 9023.

As an example, if the priority is five for a load-balancing device, it attempts to send up to six ARP packets in order to see if any master device owns the cluster IP address. If a master device is detected, the ASA does not send any more ARP messages and waits 15 seconds before it sends the UDP Hello request. The master device then responds with an UDP Hello response.

**Caveat for Reboot Scenarios**

In a reboot situation with two ASAs in a load-balancing cluster:

- Either ASA-1 or ASA-2 was the master before the reboot.

- ASA-1 is rebooted.

- ASA-2 becomes the master if it was not the master previously.

- ASA-1 simply joins the cluster as a slave after reboot.

The load-balancing algorithm might be affected by a configuration of the switch where the outside interface of the cluster devices are connected also. For example, a Spanning-Tree algorithm might cause connectivity delay when the device that is connected to the switch is rebooted.

   **Tip:** The \texttt{spanning-tree port fast} command helps to speed up the process.

In some cases, a newly rebooted ASA that has load balancing enabled might attempt to become the master device (even if a master device already exists) because it cannot reach the current master device due to a connectivity delay in the switch. When there is a mastership conflict detected as a result of ARP collision, the ASA with a low Media Access Control (MAC) address wins, while the ASA with a higher MAC address gives up the master device role.

**Master Reelection Process**

There are two situations that cause a reelection of the master device.
Master Device Removed from the Cluster

When you disable the feature on the ASA, a broadcast message is sent to all of the cluster members in order to inform of the change, and the previously described election process is performed.

Master Device does Not Respond to Cluster Member Hello Messages

If the master device does not respond to a cluster member Hello message, it takes an ASA cluster member approximately 20 seconds to detect that the master is no longer present. The Hello messages are sent every five seconds (not configurable). If cluster members do not receive a response from the master device after four Hello messages, then the election process is triggered.

Troubleshoot

Note: Refer to the Important Information on Debug Commands Cisco article before you use debug commands.

These debug commands can be useful with attempts to troubleshoot issues with your system:

- **debug fsm 255** - Use this command in order to activate the general Finite State Machine debug. Enter the no debug all command in order to deactivate.

- **debug menu vpnlb 3** - Use this command in order to activate the VPN load balancing debug trace. Enter the debug menu vpnlb 3 command once again in order to deactivate.

- **debug menu vpnlb 4** - Use this command in order to activate the VPN load balancing function trace. Enter the debug menu vpnlb 4 command once again in order to deactivate.

Related Information

- [Understanding Load Balancing](#)
- [Technical Support & Documentation - Cisco Systems](#)