Site-To-Site VPN Configuration on the Multiple Context ASA 9.x Receives Error Message

Contents

Introduction

This document describes how to troubleshoot the error mesage, "The maximum tunnel count allowed has been reached", when you configure a Site-To-Site VPN on the Multiple Context Adaptive Security Appliances (ASA) 9.x.

Prerequisites

Components Used

The information in this document is based on ASA Software Version 9.0 and later. This version introduced Site-To-Site VPN configuration in multiple context mode.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

When you attempt to bring up multiple Site-To-Site VPN tunnels on the ASA, it fails and generates the syslog message "The maximum tunnel count allowed has been reached".

The specific syslog message is below:

```
%ASA-4-751019: Local:<LocalAddr> Remote:<RemoteAddr> Username:<username> Failed to obtain a
<licenseType> license.
```

- <LocalAddr> - Local Address for this connection attempt
- <RemoteAddr> - Remote peer address for this connection attempt
- <username> - Username for peer attempting connection
- <licenseType> - License type that was exceeded (Other VPN or AnyConnect Premium/Essentials)

Background Information

The log indicates that a session creation failed because the maximum license limit for VPN tunnels was exceeded which causes a failure to either initiate or respond to a tunnel request.

The implementation of VPN in multiple-mode requires the division of the total available VPN licenses among the configured contexts. The ASA administrator can configure how many licenses each context is allocated.

By default, no VPN tunnel licenses are allocated to the contexts, and the allocation of the license type must be done manually by the administrator.

Recommended Action

Ensure enough licenses are available for all allowed users and/or obtain more licenses to allow the rejected connections. For multi-context, allocate more licenses to the context which reported the failure, if possible.

Solution

Dividing the licenses among the contexts is done by the augmentation of the resource manager with a 'VPN other' resource that manages the division of the 'Other VPN' license pool used for site-to-site VPN among the configured contexts.

The limit-resource CLI below allows this configuration within the resource 'class' mode.

```
Limit-resource vpn [burst] other <value> | <value>%
```

Where, <value> range: 1- Platform license limit or 1-100% of installed licenses.

For bursts, the range is 1 to unassigned licenses or 1-100% of unassigned licenses.
Default: 0; no VPN resources are allocated to a class.

In order to assign a context to 10% of the installed licenses, you need to define a resource class. Next, apply the class to contexts that you need to be able to get this resource within the system context configuration.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 10%
```

In order to assign a context of 250 VPN Peers of the installed licenses, you need to define a resource 'class'. Next, apply the class to the contexts that you prefer to be able to get this resource within the system context configuration.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 250
```

In order to apply the above class "vpn" to a context called "administrator", follow these steps:

1. Change/Switchover to the system context and apply the class VPN for the context "administrator". This could be done only within the System context.
2. Below is the configuration snippet to allocate the class "vpn" to the context "administrator".
   ```
   ciscoasa(config)# context administrator
   ciscoasa(config-ctx)# member vpn
   ```

Related Information

- **Cisco ASA 5500 Series Next Generation Firewalls Reference Guides**
- **Cisco ASA 5500 Series Next Generation Firewalls Configuration Guides**
- **Technical Support & Documentation - Cisco Systems**