New Features in Cisco ASA version 8
October 20, 2008
By Keith Barker

Often, I am asked about the differences between ASA5500 series firewall software version 7.x and version 8.x. This article will point out a few of the key differences, and include some sample configurations. The most noticeable feature new to version 8 is the support of EIGRP. This is configured the same way it is on an IOS router:

ASA(config)# **router eigrp 1**
ASA(config-router)#**network 10.0.0.0**
ASA(config-router)#**no auto-summary**

Another new aspect of version 8.x is that NAT can be performed even when the firewall is in transparent mode. Also the GUI of the ASA Device Manager (ASDM) has changed. It is more visually appealing than its predecessor, which is nice, but once you get used to the menus being slightly rearranged, the basics of configuring the ASA with ASDM are the same as it was in the prior version.

Many of the "behind the scenes" improvements for version 8.x went into the SSL VPN component. Cisco's latest SSL client, named AnyConnect, can be loaded onto the ASA and download/installed for authenticated remote users on demand. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections. This makes it very simple to deploy in large (and small) environments.

The AIP module, which is available for the 5500 series, performs Intrusion Detection/Prevention Services in conjunction with the ASA. The IPS module has the ability to perform as multiple virtual sensors (4 being the max). Unfortunately, these virtual sensors could not be independently assigned to separate ASA contexts (virtual firewalls), until now. Version 8.x of the ASA code supports allocating a specific virtual sensor to a single virtual firewall. The configuration, shown from the system execution space on the ASA, illustrates how to assign a virtual sensor named VS1 to the virtual firewall named VF1:

ASA(config)# **context VF1**
ASA(config-ctx)# **allocate-interface gigabitethernet0/1**
ASA(config-ctx)# **allocate-interface gigabitethernet0/0**
ASA(config-ctx)# **allocate-ips VS1**

Once the sensor has been assigned to VF1, the Modular Policy Framework (MPF) needs to be used within the virtual firewall (VF1) to direct the traffic to the senor (VS1) for analysis. In the example, all traffic destined for the IP address of 24.234.2.10 will be sent to the sensor, inline, for analysis. If the sensor fails, the traffic will not be forwarded.

ASA(config-ctx)# **changeto context VF1**
ASA/VF1(config)# **access-list IPS_ACL permit ip any host 24.234.2.10**
ASA/VF1(config)# **class-map IPS_CLASS**
ASA/VF1(config-cmap)# **match access-list IPS_ACL**
ASA/VF1(config-cmap)# **exit**
ASA/VF1(config)# **policy-map IPS_POLICY**
ASA/VF1(config-pmap)# **class IPS_CLASS**
ASA/VF1(config-pmap-c)# **ips inline fail-close**
ASA/VF1(config-pmap-c)# **exit**
ASA/VF1(config-pmap)# **exit**
ASA/VF1(config)# **service-policy IPS_POLICY interface outside**
ASA/VF1(config)#

Some of the most recent releases of the 8.x code is only for the higher end 5500 devices, such as the 5580. In time, these versions will also be available on the lower end devices including the 5505 and 5510.   All in all, if you don't specifically need EIGRP or some of the other enhancements to version 8, you may want to wait, and allow someone else to discover what bug fixes may be in store.

Article Source: http://www.ccbootcamp.com/support-resources/resources/articles-by-ccbootcamp.html