Konfigurieren der Shun-Funktion von Cisco ASA zum Befreien virtueller Appliances

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Cisco ASA konfiguriert wird, um die virtuelle Appliance von der Komponente zur Erkennung von Sicherheitsrisiken zu befreien. Die Cisco ASA-Komponente zur Erkennung von Sicherheitsrisiken führt eine Paketprüfung für DNS und andere Protokolle durch. Umbrella Support empfiehlt die folgenden ASA-Konfigurationsänderungen, um Konflikte mit dieser Funktion mit unserer virtuellen Appliance zu vermeiden:

- Befreien Sie die virtuelle Appliance von der in diesem Artikel beschriebenen "Shun"-Funktion der Bedrohungserkennung.
- Befreien Sie die virtuelle Appliance von der DNS-Paketprüfung, um unsere DNS-Verschlüsselung (DNScrypt) zuzulassen, die in diesem Artikel behandelt wird: Die Cisco ASA Firewall blockiert DNScrypt.

"Shun"-Funktion zur Erkennung von Bedrohungen

Wenn die Shun-Funktion aktiviert ist, kann die ASA eine Quell-IP-Adresse vollständig blockieren, die Regeln zur Erkennung von Sicherheitsrisiken auslöst. Weitere Informationen finden Sie im folgenden Cisco Artikel: Funktionen und Konfiguration der ASA-Bedrohungserkennung.

Die virtuelle Appliance sendet normalerweise eine sehr hohe Anzahl von DNS-Abfragen an Umbrella DNS Resolver. In Fällen, in denen bei der Verbindung mit den Resolvern ein lokales Problem auftritt (z. B. ein vorübergehender Netzwerkausfall bzw. eine vorübergehende Netzwerklatenz), können diese Abfragen fehlschlagen. Aufgrund der schieren Anzahl der gesendeten Anfragen führt bereits ein kleiner Prozentsatz der ausgefallenen Anfragen dazu, dass die ASA die virtuelle Appliance nicht verwendet. was zu einem vollständigen DNS-Ausfall für einen bestimmten Zeitraum führt.

Virtuelle Appliance ausnehmen

Anmerkung: Die Befehle in diesem Artikel dienen nur zur Orientierung. Es wird empfohlen, sich vor der Änderung einer Produktionsumgebung mit einem Experten von Cisco in

Verbindung zu setzen.

Über CLI:

- Führen Sie den folgenden Befehl aus, um zu verhindern, dass die Appliance-IP gemieden wird: **no shun**

Über ASDM-Schnittstelle:

- Wählen Sie im Bereich Configuration > Firewall > Threat Detection (Konfiguration > Firewall > Bedrohungserkennung) aus.
- Um die Appliance-IP-Adresse nicht zu vermeiden, geben Sie eine Adresse in das Feld "Netzwerke, die vom Shun ausgeschlossen sind" ein. Sie können mehrere Adressen oder Subnetze durch Kommas getrennt eingeben.

Stellen Sie fest, ob die Appliance "gemieden" wurde.

Wenn diese Schritte nicht befolgt wurden, kann die Appliance unter bestimmten Umständen "gemieden" werden, was zu einem DNS-Ausfall führt.

Wenn die virtuelle Appliance über keine externe Verbindung verfügt, protokolliert die Cisco ASA-Konsole das Ereignis wie folgt:

4|Juni 2014 14:00:42|401004: Shunned Packet: 192.168.1.3 ==> 208.67.222.222 an Schnittstelle innen
4|Juni 2014 14:00:42|401004: Shunned Packet: 192.168.1.3 ==> 208.67.222.222 (Schnittstelle innen)

Führen Sie den folgenden Befehl auf dem ASA-Gerät aus, um eine Liste der derzeit nicht verwendeten IP-Adressen anzuzeigen: **show shun**

Führen Sie den folgenden Befehl auf dem ASA-Gerät aus, um die derzeit verbotenen IP-Adressen sofort zu löschen: **clear shun**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.