Ermitteln des von der NBAR nicht erkannten Datenverkehrs

Inhalt

Einführung

In diesem Dokument wird gezeigt, wie die PDLM-Funktion (Custom Packet Description Language Module) der Network-Based Application Recognition (NBAR) verwendet wird, um nicht klassifizierten Datenverkehr oder Datenverkehr, der nicht speziell als Übereinstimmungsprotokollanweisung unterstützt wird, zu vergleichen.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- Grundlegende QoS-Methoden
- Grundlegendes Verständnis von NBAR

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.2(2)T
- Cisco 7206-Router

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Benutzerdefinierter PDLM

NBAR unterstützt eine Vielzahl von statischen und Stateful-Protokollen. PDLMs ermöglichen die Unterstützung neuer Protokolle für NBAR, ohne dass ein IOS-Release-Upgrade und ein erneutes Laden des Routers erforderlich sind. Nachfolgende IOS-Versionen beinhalten Unterstützung für diese neuen Protokolle.

Mit dem benutzerdefinierten PDLM können Sie Protokolle dem statischen User Datagram Protocol (UDP) und den TCP-Ports für Protokolle zuordnen, die derzeit in NBAR nicht mit einer Übereinstimmungsprotokollanweisung unterstützt werden. Mit anderen Worten, sie erweitert oder verbessert die Liste der von NBAR erkannten Protokolle.

Im Folgenden finden Sie die Schritte zum Hinzufügen des benutzerdefinierten PDLM zu Ihrem Router.

1. Laden Sie die NBAR-PDLM von der Software Download-Seite (nur registrierte Kunden) herunter, indem Sie die **Datei custom.pdlm herunterladen**.
2. Laden Sie das PDLM mithilfe des nachstehenden Befehls auf ein Flash-Speichergerät, z. B. eine PCMCIA-Karte in Steckplatz 0 oder 1.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Überprüfung der Unterstützung für benutzerdefinierte Protokolle mithilfe der **show ip nbar port-map | schließen den benutzerdefinierten** Befehl (siehe unten) oder den Befehl **show ip nbar pdlm ein**.
   ```
   7206-16# show ip nbar port-map | include custom
   port-map custom-01            udp 0
   port-map custom-01            tcp 0
   port-map custom-02            udp 0
   port-map custom-02            tcp 0
   port-map custom-03            udp 0
   port-map custom-03            tcp 0
   port-map custom-04            udp 0
   port-map custom-04            tcp 0
   port-map custom-05            udp 0
   port-map custom-05            tcp 0
   port-map custom-06            udp 0
   port-map custom-06            tcp 0
   port-map custom-07            udp 0
   port-map custom-07            tcp 0
   port-map custom-08            udp 0
   port-map custom-08            tcp 0
   port-map custom-09            udp 0
   port-map custom-09            tcp 0
   port-map custom-10            udp 0
   port-map custom-10            tcp 0
   ```
4. Weisen Sie den benutzerdefinierten Protokollen Ports mithilfe des Befehls **ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}** Ports zu. Um beispielsweise den Datenverkehr am TCP-Port 8877 abzugleichen, verwenden Sie den Befehl **ip nbar port-map custom-01 tcp 8877**.

Klassifizierung von "nicht klassifizierten" Ports

Abhängig von Ihrem Netzwerkverkehr müssen Sie möglicherweise spezielle Klassifizierungsmechanismen in NBAR verwenden. Nach der Klassifizierung des Datenverkehrs können Sie dann das benutzerdefinierte PDLM verwenden und die UDP- und TCP-Portnummern einer benutzerdefinierten Portzuordnung zuordnen.

Standardmäßig sind die nicht klassifizierten NBAR-Mechanismen nicht aktiviert. Der Befehl **show ip nbar unrestricted-port-stats** gibt die folgende Fehlermeldung zurück:

```
d11-5-7206-16# show ip nbar unclassified-port-stats
Port Statistics for unclassified packets is not turned on.
```

Verwenden Sie unter sorgfältig kontrollierten Umständen den Befehl **debug ip nbar unrestricted-port-stats**, um den Router so zu konfigurieren, dass er die Verfolgung der Ports durchführt, an die Pakete eingehen. Verwenden Sie dann den Befehl **show ip nbar unrestricted-port-stats**, um die erfassten Informationen zu überprüfen. Die Ausgabe zeigt nun ein Histogramm der am häufigsten verwendeten Ports an.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle. Die Befehle **debug ip nbar** sollten nur unter sorgfältig kontrollierten Umständen aktiviert werden.

Wenn diese Informationen nicht ausreichen, können Sie die Erfassungsfunktion aktivieren, die eine einfache Möglichkeit bietet, Paketspuren neuer Protokolle zu erfassen. Verwenden Sie die folgenden **Debugbefehle**, wie unten gezeigt.

```
debug ip nbar filter destination_port tcp XXXX
debug ip nbar capture 200 10 10 10
```

Der erste Befehl definiert die Pakete, an denen Sie interessiert sind, um sie zu erfassen. Mit dem zweiten Befehl wird NBAR in den Erfassungsmodus versetzt. Der Befehl **capture** hat folgende Argumente:

- Die Byteanzahl, die pro Paket erfasst werden soll.
- Anzahl der zu erfassenden Startpakete, d. h. die Anzahl der Pakete, die nach dem TCP/IP-SYN-Paket erfasst werden sollen.
- Die Anzahl der zu erfassenden Pakete, d. h. die Anzahl der Pakete am Ende des Datenflusses, für die Speicherplatz reserviert werden soll.
- Anzahl der zu erfassenden Gesamtpakete

Hinweis: Bei Angabe der Start- und Endparameter werden nur die relevanten Pakete in einem langen Datenfluss erfasst.

Verwenden Sie den Befehl **show ip nbar capture**, um die erfassten Informationen anzuzeigen. Der Erfassungsmodus wartet standardmäßig auf das Eintreffen eines SYN-Pakets und beginnt dann mit der Erfassung der Pakete in diesem bidirektionalen Fluss.

Blockieren von Gnutella mit dem benutzerdefinierten PDLM

Sehen wir uns ein Beispiel für die Verwendung des benutzerdefinierten PDLM an. Wir verwenden Gnutella als Datenverkehr, den wir klassifizieren möchten, und wenden dann eine QoS-Richtlinie an, die diesen Datenverkehr blockiert.

Gnutella verwendet sechs bekannte TCP-Ports: 6346, 6347, 6348, 6349, 6355 und 5634. Andere Ports können erkannt werden, wenn Pongs empfangen werden. Wenn Benutzer andere Ports für die Gnutella-Dateifreigabe angeben, können Sie diese Ports der benutzerdefinierten Protokollanweisung für Übereinstimmung hinzufügen.

Im Folgenden finden Sie die Schritte zum Erstellen einer QoS-Service-Richtlinie, die den Gnutella-Datenverkehr abgleicht und verwirft.

1. Verwenden Sie, wie oben erwähnt, den Befehl **show ip nbar unrestricted-port-stats**, um den "nicht klassifizierten" NBAR-Datenverkehr anzuzeigen. Wenn Ihr Netzwerk Gnutella-Datenverkehr überträgt, wird die Ausgabe ähnlich wie folgt angezeigt:
   ```
   Port    Proto    # of Packets
   ------- -------- -------
   6346    tcp      347679
   27005   udp      55043
   ```
2. Mit dem **benutzerdefinierten** Befehl **ip nbar port-map** können Sie eine benutzerdefinierte Port-Map definieren, die mit den Gnutella-Ports übereinstimmt.

   ```
   ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
   ```
   Hinweis: Derzeit müssen Sie einen Namen wie custom-xx verwenden. Benutzerdefinierte Namen für benutzerdefinierte PDLMs werden in einer kommenden Version der Cisco IOS Software unterstützt.
3. Verwenden Sie den Befehl **show ip nbar protocol stats**, um Übereinstimmungen mit der benutzerdefinierten Anweisung zu bestätigen.
   ```
   2620# show ip nbar protocol stats byte-count
   FastEthernet0/0
                  Input                Output
   Protocol       Byte Count           Byte Count
   -----------------------------------------------
   custom-02      43880517             52101266
   ```
4. Erstellen Sie mithilfe der Befehle der modularen QoS-CLI (MQC) eine QoS-Dienstrichtlinie.
   ```
   d11-5-7206-16(config)# class-map gnutella
   d11-5-7206-16(config-cmap)# match protocol custom-02
   d11-5-7206-16(config-cmap)# exit
   d11-5-7206-16(config)# policy-map sample
   d11-5-7206-16(config-pmap)# class gnutella
   d11-5-7206-16(config-pmap-c)# police 1000000 31250 31250 conform-action
                drop exceed-action drop violate-action drop
   ```

   Weitere Konfigurationsbefehle zur Blockierung von Gnutella und anderem unerwünschten Datenverkehr finden Sie unter Verwenden von Network-Based Application Recognition and Access Control Lists zum Blockieren des "Code Red"-Wurms.

Zugehörige Informationen

- QoS-Support-Ressourcen
- Technischer Support - Cisco Systems