Het verkeer bepalen niet herkend door NBAR

Inhoud

Inleiding

Dit document toont hoe de optie Aangepaste Packet Description Language Module (PDLM) van Network-Based Application Recognition (NBAR) moet worden gebruikt om op niet-geclassificeerd verkeer of verkeer te passen dat niet specifiek wordt ondersteund als een overeenkomend protocol-verklaring.

Voorwaarden

Vereisten

Lezers van dit document zouden kennis moeten hebben van deze onderwerpen:

- Basismethoden voor QoS
- Basisbegrip van NBAR

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®-softwarerelease 12.2(2)T
- Cisco 7206 router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

De aangepaste PDLM begrijpen

NBAR ondersteunt een verscheidenheid aan statische en stateful protocollen. PDLM's maken nieuwe protocolondersteuning voor NBAR mogelijk zonder dat een IOS-release en een routerherlading nodig zijn. Volgende IOS-releases biedt ondersteuning voor deze nieuwe protocollen.

Met de Aangepaste PDLM kunt u protocollen aan statische User Datagram Protocol (UDP) en TCP-poorten in kaart brengen voor protocollen die momenteel niet in NBAR met een overeenkomend protocol worden ondersteund. Met andere woorden: de lijst van door NBAR herkende protocollen wordt verlengd of uitgebreid.

Hier zijn de stappen om de Aangepaste PDLM aan uw router toe te voegen.

1. Pak de NBAR PDLM vast en download van de softwaredownpagina (alleen geregistreerde klanten) door het **aangepaste.pdf-bestand** te downloaden.
2. Laad de PDLM op een flash-geheugenapparaat, zoals een PCMCIA-kaart in sleuven 0 of 1, met behulp van de onderstaande opdracht.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Controleer de ondersteuning voor aangepaste protocollen met behulp van de **show ip-nbar poort-map | omvat** de **aangepaste** opdracht (zie hieronder) of de opdracht **ip nbar PDM**.
   ```
   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. Wijs poorten aan de aangepaste protocollen toe die de **ip** nbar **port-map op douane-XY {tcp|udp} {port1 port2 ..}** opdracht gebruiken. Bijvoorbeeld, om op verkeer op TCP haven 8877 aan te passen, gebruik de **ip nbar haven-kaart aangepaste 01 tcp 8877** opdracht.

"Niet-gerubriceerde" poorten

Afhankelijk van uw netwerkverkeer, kunt u speciale classificatiemechanismen in NBAR moeten

gebruiken. Zodra u dit verkeer classificeert, kunt u dan de aangepaste PDLM gebruiken en de UDP en TCP poortnummers aan een aangepaste haven-kaart aanpassen.

Standaard worden de NBAR niet-gerubriceerde mechanismen niet ingeschakeld. De opdracht ip **nbar unclassificeerde poort-stats** geeft de volgende foutmelding terug:

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

Onder zorgvuldig gecontroleerde omstandigheden, gebruik het **debug ip nbar niet-geclassificeerd-port-stats** bevel om de router te vormen om te beginnen bij het volgen op welke poorten die pakketten aankomen. Gebruik vervolgens de opdracht **Show ip nbar unGerubriceerde poort-stats** om de verzamelde informatie te verifiëren. De output toont nu een histogram van de meest gebruikte poorten.

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over Debug Commands. De opdrachten **debug ip** moeten alleen onder zorgvuldig gecontroleerde omstandigheden worden ingeschakeld.

Als deze informatie niet voldoende is, kunt u de opnamefunctie inschakelen, wat een makkelijke manier biedt om pakketsporen van nieuwe protocollen op te nemen. Gebruik de volgende **debug** opdrachten, zoals hieronder wordt getoond.

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

De eerste opdracht definieert de pakketten waarin u geïnteresseerd bent om op te nemen. De tweede opdracht zet NBAR in opnamemodus. De argumenten van de **opdracht** van de **opname** zijn als volgt:

- Aantal bytes per pakket opnemen
- Aantal te vangen pakketten, met andere woorden, hoeveel pakketten te vangen na het TCP/IP SYN-pakket.
- Aantal uiteindelijke pakketten die moeten worden opgeslagen, in andere woorden, hoeveel pakketten aan het eind van de stroom waarvoor ruimte moet worden gereserveerd.
- Aantal totale pakketten die moeten worden opgenomen.

Opmerking: door het specificeren van de begin- en eindpakketparameters worden alleen de relevante pakketten in een lange stroom opgenomen.

Gebruik de opdracht **om de** verzamelde informatie op **te** nemen in **de** showip nbar. De standaardinstelling is dat de opnamemodus wacht tot een SYN-pakket arriveert en vervolgens de pakketten in die bidirectionele stroom opneemt.

Gnutella blokkeren met de aangepaste PDLM

Laten we een voorbeeld bekijken van hoe we de Aangepaste PDLM kunnen gebruiken. We gebruiken Gnutella als het verkeer dat we willen classificeren en we willen een QoS-beleid toepassen dat dit verkeer blokkeert.

Gnutella gebruikt zes bekende TCP-poorten - 6346, 6347, 6348, 6349, 6355 en 5634. Andere

poorten kunnen worden gedetecteerd naarmate dieren worden ontvangen. Als gebruikers andere poorten voor gebruik in Gnutella-bestandsdeling specificeren, kunt u deze poorten toevoegen aan uw aangepaste overeenkomende protocolverklaring.

Hier zijn de stappen naar het creëren van een QoS-servicebeleid dat op Gnutella aansluit en er een daling van het Gnutella-verkeer door veroorzaakt.

1. Zoals hierboven vermeld, gebruik de opdracht van de **show ip nbar niet-geclassificeerd-port-stats** om het NBAR "niet-gerubriceerde" verkeer te bekijken. Als uw netwerk Gnutella-verkeer transporteert, ziet u uitvoer die vergelijkbaar is met de volgende.

```
Port     Proto     # of Packets
-------  --------  -------
6346     tcp       347679
27005    udp       55043
```

2. Gebruik de **ip nbar port-map aangepaste** opdracht om een aangepaste poort-map te definiëren die op de Gnutella poorten aansluit.

```
ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
```

   Opmerking: Op dit moment moet u een naam gebruiken zoals customerxx. Door gebruiker gedefinieerde namen voor aangepaste PDLM's worden ondersteund in een komende release van Cisco IOS-software.

3. Gebruik het bevel van de **het protocol van de show ip nbar** om overeenkomsten aan de douaneverklaring te bevestigen.

```
2620# show ip nbar protocol stats byte-count
FastEthernet0/0
                Input               Output
Protocol        Byte Count          Byte Count
-------------------------------------------------
custom-02       43880517            52101266
```

4. Maak een QoS-servicebeleid met de opdrachten van de modulaire QoS CLI (MQC).

```
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
```

   Raadpleeg Netwerkgebaseerde Application Recognition en toegangscontrolelijsten voor het blokkeren van het "Code Red"-werk voor andere configuratieopdrachten om Gnutella en ander ongewenst verkeer te blokkeren.

Gerelateerde informatie

- QoS-ondersteuningsbronnen
- Technische ondersteuning - Cisco-systemen