Determinazione del traffico non riconosciuto da NBAR

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Informazioni sul PDLM personalizzato](#)
[Classificazione delle porte "non classificate"](#)
[Blocco di Gnutella con il PDLM personalizzato](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene spiegato come usare la funzionalità Custom Packet Description Language Module (PDLM) di NBAR (Network-Based Application Recognition) per creare corrispondenze con traffico non classificato o non supportato in modo specifico come istruzione match protocol.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- Metodologie QoS di base
- Conoscenze base di NBAR

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.2(2)T
- Cisco 7206 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Informazioni sul PDLM personalizzato

NBAR supporta una vasta gamma di protocolli stateful e stateful. I PDLM consentono il supporto di nuovi protocolli per NBAR senza la necessità di un aggiornamento della versione IOS e di un ricaricamento del router. Le versioni IOS successive includono il supporto per questi nuovi protocolli.

Il protocollo PDLM personalizzato consente di mappare i protocolli alle porte statiche UDP (User Datagram Protocol) e TCP per i protocolli attualmente non supportati in NBAR con un'istruzione match protocol. In altre parole, estende o migliora l'elenco dei protocolli riconosciuti da NBAR.

Di seguito sono riportati i passaggi per aggiungere il file PDLM personalizzato al router.

1. Individuare e scaricare NBAR PDLM dalla pagina di download del software (solo utenti registrati) scaricando il **file custom.pdlm**.
2. Caricare il PDLM su un dispositivo di memoria flash, ad esempio una scheda PCMCIA negli slot 0 o 1, utilizzando il comando seguente.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Verificare il supporto per i protocolli personalizzati con il comando **show ip nbar port-map | include il** comando **personalizzato** (mostrato di seguito) o il comando **show ip nbar pdlm**.
   ```
   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. Assegnare le porte ai protocolli personalizzati utilizzando il comando **ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}**. Ad esempio, per verificare la corrispondenza sul traffico sulla porta TCP 8877, usare il comando **ip nbar port-map custom-01 tcp 8877**.

Classificazione delle porte "non classificate"

A seconda del traffico di rete, potrebbe essere necessario utilizzare meccanismi di classificazione speciali in NBAR. Una volta classificato questo traffico, è possibile utilizzare il PDLM personalizzato e far corrispondere i numeri delle porte UDP e TCP a una mappa delle porte personalizzata.

Per impostazione predefinita, i meccanismi non classificati NBAR non sono attivati. Il comando **show ip nbar unclassified-port-stats** restituisce il seguente messaggio di errore:

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

In circostanze attentamente controllate, usare il comando **debug ip nbar unclassified-port-stats** per configurare il router in modo che inizi a rilevare le porte da cui arrivano i pacchetti. Quindi, usare il comando **show ip nbar unclassified-port-stats** per verificare le informazioni raccolte. L'output visualizza un istogramma delle porte più comunemente usate.

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug. I comandi **debug ip nbar** devono essere abilitati solo in circostanze attentamente controllate.

Se queste informazioni non sono sufficienti, è possibile abilitare la funzionalità di acquisizione, che consente di acquisire in modo semplice le tracce dei pacchetti dei nuovi protocolli. Usare i seguenti comandi **debug**, come mostrato di seguito.

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

Il primo comando definisce i pacchetti di cui si desidera eseguire l'acquisizione. Il secondo comando attiva la modalità di cattura per NBAR. Gli argomenti del comando **capture** sono i seguenti:

- Numero di byte da acquisire per pacchetto.
- Numero di pacchetti iniziali da acquisire, in altre parole, il numero di pacchetti da acquisire dopo il pacchetto SYN TCP/IP.
- Numero di pacchetti finali da acquisire, in altre parole quanti pacchetti alla fine del flusso devono essere riservati.
- Numero totale di pacchetti da acquisire.

Nota: specificando i parametri di pacchetto iniziale e finale si acquisiscono solo i pacchetti rilevanti in un flusso lungo.

Usare il comando **show ip nbar capture** per visualizzare le informazioni raccolte. Per impostazione predefinita, la modalità di acquisizione attende l'arrivo di un pacchetto SYN e quindi avvia l'acquisizione dei pacchetti su tale flusso bidirezionale.

Blocco di Gnutella con il PDLM personalizzato

Esaminiamo un esempio di come utilizzare il PDLM personalizzato. Usiamo Gnutella come il traffico che vogliamo classificare e poi applichiamo una policy QoS che blocca questo traffico.

Gnutella utilizza sei porte TCP conosciute: 6346, 6347, 6348, 6349, 6355 e 5634. È possibile che

vengano rilevate altre porte durante la ricezione di Pong. Se gli utenti specificano altre porte da utilizzare nella condivisione dei file Gnutella, è possibile aggiungere queste porte all'istruzione personalizzata del protocollo di corrispondenza.

Di seguito vengono riportati i passaggi per creare una policy per il servizio QoS che corrisponda a Gnutella e che cessi il traffico.

1. Come accennato in precedenza, utilizzare il comando **show ip nbar unclassified-port-stats** per visualizzare il traffico "non classificato" NBAR. Se la tua rete sta trasportando il traffico Gnutella, vedrai un output simile al seguente.
```
Port    Proto    # of Packets
------- -------- -------
6346    tcp      347679
27005   udp      55043
```
2. Usare il comando **ip nbar port-map custom** per definire una mappa della porta personalizzata che corrisponda alle porte Gnutella.

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

   Nota: attualmente è necessario utilizzare un nome quale custom-xx. I nomi definiti dall'utente per i PDF personalizzati saranno supportati in una delle prossime versioni del software Cisco IOS.
3. Utilizzare il comando **show ip nbar protocol status** per confermare le corrispondenze con l'istruzione personalizzata.
```
2620# show ip nbar protocol stats byte-count
FastEthernet0/0
               Input                Output
Protocol       Byte Count           Byte Count
-----------------------------------------------
custom-02      43880517             52101266
```
4. Creare un criterio del servizio QoS utilizzando i comandi di MQC (Modular QoS CLI).
```
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
```

   Per ulteriori comandi di configurazione per bloccare Gnutella e altro traffico indesiderato, fare riferimento a Utilizzo di elenchi di riconoscimento e controllo degli accessi delle applicazioni basate sulla rete per il blocco del worm "Code Red".

Informazioni correlate

- Risorse di supporto QoS
- Supporto tecnico – Cisco Systems