Verschillen tussen Logs en Debugs op adaptieve security applicaties

Inhoud

Inleiding

Dit document biedt een eenvoudige beschrijving van de zuiveringsfunctie in Adaptieve security applicaties (ASA's) die versie 8.4 en hoger uitvoeren. Sommige functies zijn echter alleen beschikbaar in versie 9.5(2) en hoger.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- ASA 5506-X met ASA-software versie 9.5(2)
- Cisco Adaptieve Security Adapter Manager (ASDM) versie 7.5.2

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.

Basisfuncties voor vastlegging

ASA's behandelen debug-berichten anders dan Cisco IOS®-apparaten. Standaard (tenzij "logging debug-trace", wat later wordt beschreven, wordt gebruikt), worden ze op het scherm weergegeven, terwijl u via de console-poort of via telnet/Secure Shell (SSH) bent aangesloten, maar ze zijn volledig onafhankelijk. Wanneer u de console gebruikt, verschijnen ze onmiddellijk

nadat u de debug opdracht hebt ingevoerd. De zelfde actie gebeurt ook met een SSH zitting.

Onafhankelijkheid betekent dat wanneer u uiteinden op de troostpoort toestaat en u door SSH wordt verbonden, de uiteinden niet op SSH verschijnen. U dient deze handmatig opnieuw in te schakelen. Als debugs ook op één SSH-sessie zijn ingeschakeld, verschijnen ze helemaal niet op de andere sessie. U kunt het als **per sessie** doorverwijzen.

Er is ook geen behoefte om het bevel van de **eindmonitor** op een ASA in te voeren om details te tonen, omdat de uiteinden die op SSH of een telnet zitting worden toegelaten ongeacht deze opdracht verschijnen. Het doel van deze opdracht is veel anders dan in Cisco IOS-apparaten en ASA Configuration Voorbeeld beschrijft deze functie in detail.

Verschil tussen slogan- en debug-berichten

De debugs zijn gespecificeerde berichten voor een bepaald protocol of een bepaalde functie van ASA's. Er is geen niveau van debugs, maar ze zijn zeer gedetailleerd en het detailniveau kan worden gewijzigd. Ze hebben misschien ook geen tijdstempel, berichtcode of ernst. Dit is afhankelijk van het specifieke debug.

Dit voorbeeld laat het verschil zien tussen debugs en syslog boodschappen met betrekking tot hetzelfde ping verzoek.

Dit is een voorbeeld van het zuiveren van uitvoer nadat u de opdracht **debug icmp Tracker** hebt ingevoerd:

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

Dit is een voorbeeld van een syslog-bericht met betrekking tot hetzelfde ICMP-verzoek:

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Verzamelen van uitwerpselen

De standaard tijd voor SSH of telnet is vijf minuten en de sessie wordt losgekoppeld na deze tijd van inactiviteit. De standaard tijdelijke oplossing voor consoleverbinding is 0, wat betekent dat de gebruiker inlogt tot de gebruiker handmatig uitlogt.

Helaas is de logoptie beperkt door de tijd die op een bepaalde beheermethode is ingesteld, dus als de SSH-sessie eindigt, stoppen de debugs ook.

Als u de debugs gedurende langere tijd wilt verzamelen, moet u de console-verbinding gebruiken en dan kunt u ze doorsturen naar de sylogserver met de opdracht **debug-sporen**. Ze worden doorgestuurd als syslobericht 711001, afgegeven op ernst niveau 7. Om te stoppen met het verzenden van deze berichten naar logs, kunt u "nee" vóór de opdracht gebruiken.

```
logging debug-trace
no logging debug-trace
```

Vanaf versie 9.5.2 kunt u met de ASA debugs blijven verzenden als syslig-berichten na een onderbreking of log out op een SSH/telnet/console-verbinding. Als u de opdracht **debug-spoorpersistentie** invoert, kunt u selectief uiteinden die in één sessie zijn ingeschakeld, uit een andere sessie verwijderen en blijven ze actief op de achtergrond. Om deze optie uit te schakelen, plaatst u "nee" vóór de opdracht.

```
logging debug-trace persistent
no logging debug-trace persistent
```

Standaard dienen alle debug-berichten een ernst van niveau 7 te hebben. Om ze te filteren uit ongewenste berichten, kunt u de ernst van dit bericht naar 3 verhogen zodat u alleen foutmeldingen naast de apparaten verzamelt. Typ "nee" om deze omleiding uit te schakelen.

```
logging message 711001 level 3
no logging message 711001 level 3
```

Monsterconfiguratie

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

Met deze opdrachten kunt u foutmeldingen en ICMP-versies (Internet Control Message Protocol) verzenden die ook als fouten in de syslogserver worden gemarkeerd:

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Gerelateerde informatie

- ASA IPS-configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems