Fehlerbehebung bei Datenverkehrsproblemen mit der CSF-CLI

Inhalt

Einleitung

In diesem Dokument wird die Verwendung der Cisco Secure Firewall CLI zur Behebung von Datenverkehrsproblemen durch die Validierung von Routing, Paketfluss und Snort-Verhalten beschrieben.

Voraussetzungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Management Center (FMC)-Richtlinien und -Objektkonfiguration

- Cisco Secure Firewall (CSF)-Routing und -Schnittstellenlogik
- Konzepte zur Fehlerbehebung bei Paketprüfungen und Firewalls

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen für CSF beschränkt. Auf dem im Dokument verwendeten Gerät wird Code 7.6.5 ausgeführt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Secure Firewall Management Center (FMC)
- Cisco Secure Firewall (CSF)
- Firepower Threat Defense CLI-Tools

Wichtige Informationen

Bei einer erhöhten CPU-, Arbeitsspeicher- oder E/A-Auslastung kann die Ausführung von Befehlen zur Fehlerbehebung die Leistung beeinträchtigen. Es wird empfohlen, zuerst den Zustand der Ressourcenauslastung zu untersuchen und zu beheben und dann mit der Diagnose von Datenverkehrsproblemen fortzufahren. Diagnosebefehle verbrauchen zusätzliche Systemressourcen, was die Verfügbarkeit weiter beeinträchtigen und die Wiederherstellungszeit verlängern kann.

Hintergrundinformationen

Die Fehlerbehebung für den Datenverkehr auf CSF beginnt häufig mit der Bestätigung des logischen Pfads, den ein Paket durch die Firewall nehmen muss. Sobald die Route und die Schnittstellenzuordnung verstanden wurden, besteht der nächste Schritt darin, den erwarteten Pfad mit dem tatsächlichen Paketfluss zu vergleichen. Dies kann mithilfe von Routensuchvorgängen, der Paketverfolgungssimulation, der Paketerfassung und der Snort Engine-Verfolgung erfolgen.

Jedes Tool bietet eine andere Transparenz-Ebene:

- show route bestätigt den Routing-Pfad und die Schnittstellenidentität des Pakets.
- Der Paket-Tracer simuliert den Datenverkehrsfluss und identifiziert ACL-, NAT- und Schnittstellenentscheidungen.
- Paketerfassung prüft Live-Datenverkehr, der die Firewall passiert.
- System Support Trace macht Snort-Entscheidungen für richtlinienbezogene Blöcke oder Inspektionsereignisse verfügbar.

Tipp: Beginnen Sie mit der Validierung von Routing und Packet-Tracer, bevor Sie Datenverkehr erfassen. So können Sie vor der Analyse von Live-Datenverkehr überprüfen, ob die erwarteten Entscheidungen zur Pfad- und Zugriffskontrolle richtig sind.

Problem

Ein Datenverkehrsfluss funktioniert nicht wie erwartet, und der Administrator muss feststellen, ob das Paket den richtigen Pfad einnimmt, ob die Firewall die Verbindung zulässt oder verweigert und ob die Snort- oder Richtlinienprüfung den Datenverkehr blockiert.

Schritt 1: Routensuche

Identifizieren Sie den Routing-Pfad und bestimmen Sie die logischen Schnittstellennamen, die mit der Quell- und Ziel-IP-Adresse verknüpft sind. Die logischen Schnittstellennamen werden von den meisten Befehlen zur Fehlerbehebung benötigt. Daher muss dies der erste Schritt im Workflow zur Fehlerbehebung sein.

Führen Sie den Befehl für die Quell- und Ziel-IP-Adresse aus:

```
show route <IP>
```

Für den Internetdatenverkehr, der auf der Standardroute beruht, muss die logische Ausgangsschnittstelle identifiziert werden. Der Name der logischen Schnittstelle kann durch Ausführen dieses Schritts bestimmt werden:

```
show route 0.0.0.0
```

Beispiel:

```
FTD1# show route 192.168.0.11


Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

In diesem Beispiel ist die logische Eingangsschnittstelle Inside (Intern) und die Ausgangsschnittstelle Outside (Außen).

Vorsicht: Network Address Translation (NAT) kann Datenverkehr über andere Schnittstellen umleiten, wenn die NAT-Richtlinien mit dem Datenverkehrsfluss übereinstimmen. Wenn Sie Verbindungsfehler beheben, stellen Sie sicher, dass Ihre NAT-Konfiguration mit dem erwarteten Datenverkehrspfad übereinstimmt.

Tipp: Die logischen Schnittstellennamen werden in CLI-Befehlen zur Fehlerbehebung verwendet. Notieren Sie sich den logischen Namen, um später darauf zugreifen zu können.

Phase 2: Ausführen von Packet Tracer

Mit dem Paket-Tracer simulieren Sie, wie die Firewall einen bestimmten Datenverkehrsfluss auswertet. Mit diesem Tool können Sie feststellen, welche Schnittstellen verwendet werden, ob eine NAT-Richtlinie angewendet wird und ob eine ACL den Datenverkehr zulässt oder verweigert.

Verwenden Sie diese Befehlssyntax:

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Beispielbefehl:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Überprüfen Sie die Ausgabe, um sicherzustellen, dass das Paket dem erwarteten Pfad folgt und während der Simulation zulässig ist. Dies ist nützlich, wenn Sie vor der Live-Paketanalyse feststellen müssen, ob das Problem mit Routing, NAT oder der Anpassung von Richtlinien zusammenhängt.

Das Schlüsselwort "Transmit" im Packet-Tracer veranlasst das Einschleusen des simulierten Pakets an der Eingangsschnittstelle, sodass es alle Verarbeitungsphasen der Firewall durchlaufen kann, anstatt als Simulation zu verbleiben.

Beispielbefehl:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

Schritt 3: Erfassungen ausführen

Verwenden Sie die Paketerfassung, um Live-Datenverkehr zu überprüfen, der die Firewall passiert. Die Paketerfassung unterscheidet sich von der Paketverfolgung, da sie den tatsächlichen Datenverkehr erfasst und daher mit dem tatsächlichen Datenfluss übereinstimmen muss, der zum Zeitpunkt der Erfassung die Firewall durchquert. Die Paketerfassungen erfolgen in beide Richtungen und dokumentieren beide Seiten der Verbindung.

Konfigurieren Sie für die meisten Fehlerbehebungsszenarien für den Datenverkehr die folgenden Erfassungen:

- Eingangserfassung - Erfasst den an der Quellschnittstelle eingehenden Datenverkehr
- Egress Capture: Erfasst den Datenverkehr, der an der Schnittstelle auf der Zielseite zurückgeht
- ASP Drop Capture: Erfasst Pakete, die von der Firewall verworfen werden und den konfigurierten Kriterien entsprechen.

Allgemeine Erfassungssyntax:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Beispiel für Eingangserfassung:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Beispiel für Ausgangserfassung:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Beispiel für ASP-Drop-Erfassung:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

Die Paketerfassung ist bidirektional, d. h. sowohl der Vorwärts- als auch der Rückwärtsverkehr können auf Basis der definierten Übereinstimmungskriterien erfasst werden. Die Trace-Funktion ermöglicht eine Visualisierung der Entscheidungen, die die Firewall über den tatsächlichen Datenverkehr trifft.

⚠ Vorsicht: Wenn NAT durchgeführt wird, muss die Ausgangserfassung die umgewandelte Quell-IP und nicht die ursprüngliche Quell-IP verwenden, um den Datenverkehr nach NAT korrekt zu erfassen.

Schritt 4: Trace für den Systemsupport ausführen

Verwenden Sie den System Support Trace, um den Echtzeit-Prüfprozess von Snort für einen bestimmten Datenverkehrsfluss anzuzeigen. Dies ist besonders nützlich, wenn der Datenverkehr mit einer ACL-Zulassungsregel übereinstimmt, aber dennoch durch eine Richtlinienprüfung blockiert wird. Bei der standardmäßigen Paketerfassung wird angezeigt, dass ein Paket blockiert wurde. Der System Support Trace bietet jedoch eine Übersicht, warum das Paket auf diese Weise

behandelt wurde. Die Trace zur Systemunterstützung ist bidirektional, d. h. sie empfängt Datenverkehr von beiden Seiten. Das bedeutet, dass die Reihenfolge, in der die IPs zum Tool hinzugefügt werden, keine Rolle spielt.

Führen Sie diesen Befehl aus, und antworten Sie auf die Eingabeaufforderungen:

```
> system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Dieses Tool ist besonders hilfreich, wenn in der Umgebung Anwendungs- oder URL-Regeln, identitätsbasierte Regeln, Dateirichtlinien oder Zugriffsrichtlinien verwendet werden. Diese Funktionen werden nach der ACL-Übereinstimmung ausgewertet, sodass ein Paket von der Zugriffskontrollrichtlinie zugelassen, aber durch die Snort-Prüfung blockiert werden kann.

Anmerkung: Der Client-Port kann leer gelassen werden, wenn der genaue Quellport unbekannt ist.

Überprüfung

Verwenden Sie die Ausgabe der Route Lookup, Packet-Tracer-Simulation, Paketerfassung und System Support Trace zusammen, um das Verhalten des Datenverkehrsflusses zu bestätigen. Das Ziel besteht darin, anhand einer eingehenderen Überprüfung zu ermitteln, ob das Paket den richtigen Pfad einnimmt, ob die Firewall es zulässt oder verweigert und ob Snort es blockiert.

Ein vollständiger Fehlerbehebungsablauf bestätigt in der Regel Folgendes:

- Die Routensuche zeigt die logischen Eingangs- und Ausgangsschnittstellen an.
- Der Packet-Tracer bestätigt den beabsichtigten Weiterleitungspfad und die Richtlinienauswertung.
- Durch Paketerfassungen wird bestätigt, ob der Datenverkehr erwartungsgemäß ankommt und wieder abfließt.
- Die Systemsupportüberwachung bestätigt, ob die Blockierung durch Snort- oder

Richtlinieninspektion verursacht wird.

Fehlerbehebung

Wenn ein Datenverkehrsproblem weiterhin besteht, überprüfen Sie folgende Bereiche:

- Überprüfen Sie, ob die Routensuche mit den erwarteten Quell- und Zielschnittstellen übereinstimmt.
- Überprüfen Sie, ob die Ausgabe der Paketverfolgung den Datenverkehr anzeigt, der in der ACL- oder NAT-Phase abgelehnt wird.
- Überprüfen Sie die Eingangs- und Ausgangspaketerfassung, um sicherzustellen, dass der Datenverkehr die Firewall erreicht und an der richtigen Schnittstelle zurückbleibt.
- Verwenden Sie ASP-Drop-Captures, um zu bestätigen, ob die Firewall den Datenverkehr intern verwirft.
- Verwenden Sie die Systemsupport-Ablaufverfolgung, um festzustellen, ob Snort den Datenverkehr blockiert, nachdem die ACL-Genehmigungsentscheidung gefallen ist.

Zugehörige Informationen

- Analyse der FirePOWER-Firewall-Erfassung zur Behebung von Netzwerkproblemen
- Verwenden von FirePOWER Threat Defense-Erfassungen und Packet Tracer

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.