IDS 4.0/AIP-SSM/IPS 5.0 und spätere FAQ

Inhalt

Einführung

Dieses Dokument beantwortet die am häufigsten gestellten Fragen zu Cisco Secure Intrusion Detection System (IDS) 4.0, Advanced Inspection and Prevention Security Services Module (AIP SSM) und Cisco Intrusion Prevention System (IPS) 5.0 und höher.

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

IDS 4.0

F. Ich habe IDS MC und SecMon auf einem neuen Server installiert und möchte nun alle Konfigurationen (Benutzer, Gerät usw.) vom alten Server auf den neuen Server importieren. Wie mache ich das?

Antwort: Die einfachste Methode ist, den neuen VMS-Server aufzurufen und dann die Sensoren mit dieser neuen Box zu entdecken.

Hinweis: Fügen Sie den Sensor nicht manuell hinzu, wenn Sie ihn hinzufügen. Aktivieren Sie das Kontrollkästchen **Einstellungen erkennen**.

Nachdem der Sensor erkannt wurde, importieren Sie ihn in **SecMon**. Alle Konfigurationen werden auf dem Sensor gespeichert. Die Signatureinstellungen, Filter usw. sollten nach dem Erstellen des neuen Servers angezeigt werden. Stellen Sie sicher, dass Sie IDS MC auf die neuesten Signaturen aktualisieren.

F. IDS-4215 empfängt `idsPackageMgr: ungültige Argument`-Fehlermeldung, wenn versucht wird, die IDS-Wiederherstellungspartition zu aktualisieren. Wie kann ich dieses Problem beheben?

Antwort: Dies ist ein Herstellungsproblem. Einige Kunden erhielten IDS-4215 mit einem schlechten Basis-Image (4.0). Führen Sie diese Schritte aus.

1. Laden Sie das Wiederherstellungspartition-Image herunter (nur registrierte Kunden).
2. Führen Sie ein Upgrade des Image der Wiederherstellungspartition über die CLI durch:

```
sensor#configure terminal
sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/
    IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg
```

3. Sobald das Image der Wiederherstellungspartition angewendet wurde, wird der 4215 auf eine normale 4.1(1) 4215-Basis wiederhergestellt.
```
sensor(config)#recover application-partition
```

F. Wenn ich von einem zweistelligen auf ein dreistelliges sig-Level-Paket wie S100 oder höher (z. B. 4.1(4)S99 auf 4.1(4)S100) upgrade, schlägt die automatische Update-Funktionalität fehl. Wie kann ich das beheben?

Hinweis: Kunden von Cisco VMS und CLI haben dieses Problem nicht.

Die Ursache des Problems ist die Sortierlogik, die beim Analysieren des Dateinamens verwendet wird. Es ist eine alphanumerische Sortierung, wenn es numerisch sein soll. Die Problemumgehung besteht in der Verwendung von CLI (oder VMS) für ein Upgrade auf dreistellige SIG-Pakete wie S100 oder höher. Nach Abschluss dieses Vorgangs beginnt die automatische Aktualisierung wieder zu funktionieren. Weitere Informationen finden Sie unter Cisco Bug ID CSCef07999 (nur registrierte Kunden).

F. Worin besteht der **"Fehler bei der Manipulation von Authentifizierungstoken"?** Fehlermeldung bedeuten?

Antwort: Um dieses Problem zu beheben, verwenden Sie das Standardkennwort (cisco) zweimal und ändern Sie anschließend das Kennwort aus dem Konfigurationsmodus. Für das IDS muss das Standardkennwort zweimal eingegeben werden.

Beispiel:

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

F. Wie entferne ich das IDSM vom Switch?

Antwort: Das Modul sollte erst entfernt werden, nachdem Sie die Stromversorgung deaktiviert haben. Gehen Sie wie folgt vor:

1. Führen Sie in der Sensor-CLI den Befehl **Reset PowerDown aus**.
2. Wenn der Sensor das Herunterfahren abgeschlossen hat, geben Sie entweder den Befehl **no power enable module (module_number)** für Cisco IOS oder den Befehl **set module down (module_number)** für CatOS aus.
3. Drücken Sie die Taste zum Herunterfahren auf dem Blade.
4. Schalten Sie das Gehäuse aus. Wenn die Statusanzeige länger grün leuchtet, können Sie das Modul sicher entfernen.

IPS 5.0 und höher

F. Ich habe mich nicht konfiguriert, aber ich bin verwirrt, wie man die Blockierung auf den Signaturen konfiguriert. Worin besteht der Unterschied zwischen der Blockhost- und Blockverbindung?

Antwort: Host blockiert alle Pakete von dieser Quelladresse. Die Verbindung wird nur blockiert, wenn eine Verbindung auf der Grundlage der Quell- und Ziel-IP/Port-Adresse blockiert wird. Der PIX funktioniert etwas anders. Bei automatischen Shuns sendet der Sensor die Quell-IP, Ziel-IP, den Quell-Port und den Ziel-Port. Der PIX blockiert alle Pakete, die von dieser IP-Adresse stammen. Die zusätzlichen Informationen werden vom PIX verwendet, um diese Verbindung aus den Verbindungstabellen zu entfernen. Wenn die Verbindung nicht aus der Verbindungstabelle entfernt wurde, ist es theoretisch möglich, dass die ursprüngliche Verbindung möglicherweise noch nicht abgelaufen ist, wenn sie kurz nach der Anwendung entfernt wird. Dadurch kann der Angreifer den Angriff auf die ursprüngliche Verbindung fortsetzen. Durch das Entfernen der Verbindung aus der Tabelle wird sichergestellt, dass die ursprüngliche Verbindung nicht verwendet werden kann, um den Angriff nach dem Entfernen des Shuns fortzusetzen. Der Sensor kann eine einzelne Verbindung auf dem PIX nicht sperren, da der PIX die Verwendung des Befehls **shun** nicht unterstützt, um eine einzelne Verbindung zu schließen. Der PIX-Befehl **shun** deaktiviert immer die Quelladresse, unabhängig davon, ob die zusätzlichen Verbindungsinformationen bereitgestellt werden oder nicht.

F. Was tut der **"Fehler: Die Netzwerkservices konnten nicht neu gestartet werden. Es ist ein schwerwiegender Fehler aufgetreten. Knoten MUSS neu gestartet werden, um Alarming zu aktivieren."** Fehlermeldung bedeuten?

Antwort: Dieser Fehler bedeutet, dass das Standardgateway falsch ist oder eine allgemeine Fehlermeldung, die bedeutet, dass entweder die IP-Adresse, die Netzmaske oder das Standardgateway falsch sind. Der `fatale` Teil der Nachricht bedeutet, dass nach dem ersten Fehler die vorherige Konfiguration angewendet wurde und auch fehlgeschlagen ist. Der Sensor gibt **ifconfig**- und **route**-Befehle aus, und einer oder beide Befehle schlägt fehl.

F. Autoupdate schlägt mit der **"mainApp[343] Cid/E errSystemError http error response:500" fehl.** Fehlermeldung. Was bedeutet diese Fehlermeldung?

Antwort: Dieses Problem kann die Funktion für die automatische Aktualisierung sein, die nicht funktioniert, da sie so eingestellt ist, dass sie zu einer geraden Stunde heruntergeladen wird. Versuchen Sie, die automatische Aktualisierung auf eine zufällige Zeit einzustellen. selbst ein kleiner Offset von acht oder Nachtminuten kann dieses Problem beheben.

Im Allgemeinen wurde das Problem behoben und der `Fehler: http-Fehlerantwort: 500` Fehlermeldungen werden angezeigt, wenn Sie die Abrufzeit auf eine nicht stündliche Grenze ändern.

Hinweis: IPS schlägt die automatische Signaturaktualisierung fehl und gibt diese Fehlermeldung zurück:

```
AutoUpdate-Ausnahme: HTTP-Verbindung fehlgeschlagen [1,110] name=errSystemError
```

Überprüfen Sie die folgenden Punkte, um dieses Problem zu beheben:

- Überprüfen Sie, ob eine Firewall verhindert, dass der Sensor Cisco.com erreicht.
- Überprüfen Sie, ob das Routing zu einem Problem wird.
- Überprüfen Sie, ob NATing auf dem Gateway-Gerät für das Downstream-Gerät ordnungsgemäß konfiguriert ist.
- Überprüfen Sie, ob die Benutzeranmeldeinformationen korrekt sind.
- Ändern Sie die Startzeit für die Aktualisierung auf ungerade Stunden.

F. Was tut der **"Fehler: ExecUpgradeSoftware: AnalysisEngine ist derzeit beschäftigt und kann dieses Update nicht verarbeiten. Bitte warten Sie einige Minuten, bevor Sie erneut versuchen, die Aktualisierung durchzuführen."** Fehlermeldung bedeuten?

Antwort: Um dieses Problem zu beheben, versuchen Sie, den Sensor neu zu laden, oder erstellen Sie ein neues Image des Sensors.

F. Wie löse ich die Fehlermeldung **Cid/W Warning - DNS- oder HTTP-Proxy ist für die globale Korrelationsinspektion und Reputationsfilterung erforderlich, aber es sind keine DNS- oder Proxy-Server definiert.Fügen Sie einen HTTP-Proxy-Server oder DNS-Server in die Dienstkonfiguration des Hosts hinzu**?

Antwort: Führen Sie diese Schritte aus, um dieses Problem zu beheben:

- Globale Korrelation deaktivieren
- Fügen Sie die Proxy-/DNS-Konfiguration hinzu.

F. Wie kann ich diese Fehler beheben, die IPS bei Problemen mit dem globalen Korrelationsstatus erhält? "**23Jan2010 15:50:39.831 38.001 CollaborationApp[655] rep/E Ein globales Korrelations-Update ist fehlgeschlagen: Fehler beim Öffnen einer TLS-Verbindung mit dem HTTP-Server unter X.X.82.127:443: TLS-Verbindung fehlgeschlagen**" und "**collaborationApp[459] rep/E Ein globales Korrelations-Update ist fehlgeschlagen: Fehler beim Download von ibrs/1.1/drop/default/1296529950 : URI enthält keine gültige IP-Adresse**"?

Antwort: IPS kann aufgrund eines Port-Problems nicht auf das Internet zugreifen, z. B. eine Firewall in einem Pfad, der nicht über die richtigen Ports für den Internetzugriff verfügt, oder ein NAT-Problem.

Damit die globale Korrelation vollständig funktioniert, kontaktiert der Sensor zunächst über https **update-manifests.ironport.com**, um den Benutzer zu authentifizieren und dann eine HTTP-Verbindung, um GC-Updates herunterzuladen. Die Dateien, die der Sensor von HTTP (updates.ironport.com) herunterlädt, sind Reputationsdaten, die globale Korrelation verwendet. Die https update-manifests.ironport.com sollte immer auf die Adresse X.X.82.127 aufgelöst werden. Die IP-Adresse http **updates.ironport.com** kann sich ändern, je nachdem, auf welches Internet Sie zugreifen. Sie müssen also die IP-Adresse überprüfen. Wenn die URL-Filterung aktiviert ist, fügen Sie eine Ausnahme für die IP-Adresse der IPS-Verwaltungsschnittstelle im URL-Filter hinzu, sodass IPS eine Verbindung zum Internet herstellen kann.

Dieser Fehler tritt auf, wenn ein vorheriges GC-Update beschädigt ist:

```
collaborationApp[459] rep/E Ein globales Korrelations-Update ist fehlgeschlagen: Fehler beim
Download von ibrs/1.1/drop/default/1296529950 : Der URI enthält keine gültige IP-Adresse.
```

Dieses Problem kann in der Regel dadurch behoben werden, dass der GC-Dienst ausgeschaltet

und dann wieder eingeschaltet wird. Wählen Sie in IDM **Configuration > Policies > Global Correlation > Inspection/Reputation**, set Global Correlation Inspection (and **Reputation Filtering** if **On**) to **Off (**Globale Korrelationsüberprüfung und **Reputationsfilterung**), wenden Sie die Änderungen an, warten Sie 10 Minuten, schalten Sie die Funktionen ein, und überwachen Sie.

F. Die `Aktualisierung der globalen Korrelation ist fehlgeschlagen: openConnection: Caught IpAddrException badAddrString. Die HTTP-Proxy- und DNS-Einstellungen der Global Correlation konnten nicht verwendet werden. Überprüfen Sie die Verbindung, und versuchen Sie es erneut.` in der Kategorie "Reputation update failure" (Reputations-Update-Fehler) wird eine Fehlermeldung angezeigt. Wie kann ich dieses Problem beheben?

Antwort: Überprüfen Sie die folgenden Elemente:

- Sie benötigen eine gültige IPS-Lizenz, damit globale Korrelationsfunktionen funktionieren.
- Sie müssen über einen HTTP-Proxyserver oder einen DNS-Server verfügen, damit globale Korrelationsfunktionen funktionieren können.
- Da globale Korrelationsaktualisierungen über die Sensormanagementschnittstelle erfolgen, müssen Firewalls Datenverkehr vom Typ tcp 443/80 und udp 53 zulassen.
- Stellen Sie sicher, dass Ihr Sensor die globalen Korrelationsfunktionen unterstützt. Wenn Sie dies nicht wünschen, deaktivieren Sie die Funktion für globale Zusammenarbeit von IDM:Gehen Sie zu **Configuration** > **Policies** > **Global Correlation** > **Inspection/Reputation**, und stellen Sie Global Correlation Inspection (and Reputation Filtering if **On) auf Off (Aus).**

F. Wie kann ich das `"Update einer globalen Korrelation fehlgeschlagen: openConnection: Wird der IpAddrException badAddrString"`-Fehler `ausgegeben`, den IPS für ein globales Korrelationsgesundheitsproblem erhält?

Antwort: Wenn Sie die globale Korrelation (GC) verwenden, stellen Sie sicher, dass die Namensauflösung funktioniert, z. B. DNS erreichbar ist. Überprüfen Sie auch, ob ein durch die Firewall blockierter Port 53 vorhanden ist. Andernfalls können Sie die GC-Funktion ausschalten, wenn Sie diese Nachricht entfernen möchten.

F. Wie löse ich die `Ausnahme, wenn ich die` Fehlermeldung `Verbindung mit MySQL initialisiere`, die ich beim Start von IME vom Browser erhalte?

Antwort: Dieses Problem tritt in der Regel dann auf, wenn der Kunde versucht, IME auf nicht unterstützten Betriebssystemen wie Windows 7 auszuführen.

F. Wie löse ich den `" Titel: IDM bei 88-nsmc-c1-Anbieter: Cisco Systems, Inc. Kategorie: Launch File Error JAR Ressourcen in JNLP Datei sind nicht durch dasselbe Zertifikat signiert". oder "Fehler beim Herstellen der Verbindung zum Sensor, Fehler beim Erstellen des Sensors x.x.x.x:443 beim Beenden des Im"`-Fehlers, den IDM erhält, der beim Start der Anwendung auftritt?

Antwort: Löschen Sie den Browser-Cache, um dieses Problem zu beheben.

F. Ist der asymmetrische Modus auf IPS konfigurierbar, wenn Sie GUI verwenden?

Antwort: In Version 6.0 ist der asymmetrische Modus auf IPS konfigurierbar, der nur über die CLI

konfiguriert werden kann und auf der GUI nicht verfügbar ist. In Version 6.1 ist diese Funktion jedoch auch in der GUI verfügbar.

F. Wie kann ich das Latenzproblem mit dem IPS-Sensor beheben?

Antwort: Um dieses Problem zu beheben, aktivieren Sie die Verarbeitung des asymmetrischen Modus, damit der Sensor den Zustand mit dem Fluss synchronisieren und die Prüfung für die Motoren aufrechterhalten kann, die nicht beide Richtungen benötigen. Verwenden Sie diese Konfiguration:

```
IPS_Sensor#configure terminal
IPS_Sensor(config)#service analysis-engine
IPS_Sensor(config-ana)#virtual-sensor vs0
IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

Das Latenzproblem tritt auf, wenn die deny-Aktion inline und das deny-Paket für jede Signatur in VS0 aktiviert sind. Die Aktivierung aller Signaturen führt zu Latenz, da IPS jedes einzelne Paket überprüft, das durchläuft. Es empfiehlt sich, nur die Signatur zu aktivieren, die gemäß dem Netzwerkverkehrsfluss erforderlich ist, um das Latenzproblem zu beheben.

F. Unterstützt AIP-SSM die Blockierung von Skype?

Antwort: PIX/ASA kann den Skype-Datenverkehr nicht blockieren. Skype verfügt über die Kapazität, dynamische Ports auszuhandeln und verschlüsselten Datenverkehr zu verwenden. Bei verschlüsseltem Datenverkehr ist es nahezu unmöglich, ihn zu erkennen, da es keine Muster gibt, nach denen gesucht werden muss.

Sie können ein Cisco IPS (Intrusion Prevention System)/AIP-SSM verwenden. Es verfügt über Signaturen, die einen Windows Skype-Client erkennen können, der mit dem Skype-Server verbunden ist, um seine Version zu synchronisieren. Dies geschieht normalerweise, wenn der Client die Verbindung initiiert. Wenn der Sensor die anfängliche Skype-Verbindung abnimmt, können Sie die Person finden, die den Dienst verwendet, und alle Verbindungen blockieren, die über die IP-Adresse initiiert wurden.

F. Warum `klappen` die Sensorschnittstellen oder wechseln häufig in den Ausfallzustand des IPS?

Antwort: Während einer Signaturaktualisierung und Neukonfiguration stoppt sensorApp die Paketverarbeitung, während es die neuen Signaturen im Update verarbeitet. Der Netzwerktreiber erkennt, dass sensorApp angehalten wurde, und ruft alle neuen Pakete aus dem Puffer. Der Netzwerktreiber kann also verschiedene Aufgaben ausführen, die von der Konfiguration und dem Sensormodell abhängen:

Promiscuous Interface (**Promiscuous-Schnittstelle**) - Es führt die Verbindung auf den Schnittstellen herunter und bringt die Verbindung wieder hoch, sobald sensorApp wieder mit der Überwachung beginnt.

Inline-Schnittstelle oder Inline-VLAN-Paar - Dies hängt von der Bypass-Einstellung ab:

- **Bypass Auto (Automatisch umgehen)**: Der Treiber führt die Verbindung weiter aus und beginnt, Pakete ohne Analyse zu durchlaufen. Anschließend werden die Pakete wieder über

sensorApp gesendet, sobald sensorApp wieder mit der Überwachung beginnt.

- **Bypass Off** (**Aus**) **- Der** Treiber bringt die Verbindung auf den Schnittstellen herunter. Dies entspricht dem Promiscuous-Modus und bringt sie wieder hoch, sobald sensorApp wieder die Überwachung startet.

Wenn also die Sensor-App Pakete nicht aus dem Puffer abruft, was möglicherweise auftritt, weil keine Schnittstelle für die Verarbeitung von Paketen konfiguriert ist, kann der Treiber die Schnittstelle in einen `ausgefallenen` Zustand versetzen.

Diese Protokolle werden beim Flapping der Sensorschnittstelle angezeigt:

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

F. Verfügt der IDS- oder IPS-Sensor (Intrusion Prevention System) über einen Kennwortverlauf?

Antwort: Nein, der Sensor speichert keinen Kennwortverlauf. Kennwörter können zu keinem Zeitpunkt angezeigt werden.

F. Unterstützt der IDS- oder IPS-Sensor (Intrusion Prevention System) den Syslog-Server zum Senden von Protokollen?

Antwort: Nein.

F. Wie hoch ist der Grenzwert für das Speichern von Ereignissen in IPS?

Antwort: Das lokale Ereignis des Sensors speichert nur 30 MB und beginnt, sich selbst zu überschreiben, sobald das Limit von 30 MB erreicht ist. Dieses Limit ist nicht konfigurierbar.

F. Wie schreibe ich eine Signatur, um die foto[a-z]\.zip-Datei in einer ein- oder ausgehenden E-Mail zu erkennen?

Antwort: Verwenden Sie STRING.TCP, um eine Signatur zu schreiben, die die Anlage erkennt. Suchen Sie nach etwas Ähnlichem:

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
             [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
```

```
ServicePorts 25
StorageKey =STREAM
```

F. Wie konfigurieren Sie das FTP-Client-Timeout?

Antwort: Geben Sie folgende Befehle ein:

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

F. Wie konvertieren Sie die Startzeit und Endzeit im iplog-Status in ein lesbares Format?

Antwort: Diese Ausgabe ist eine Dezimaldarstellung der aktuellen Zeit seit UNIX Epoc. Verwenden Sie einen UNIX-Epoc-Rechner, z. B. den Rechner, der sich an der UNIX Date/Time Calculator befindet. Geben Sie die ersten 10 Ziffern ein, da dieser Rechner in nur Sekunden granular ist und das IDS Nanosekunden speichert. Dies bedeutet, dass die letzten neun Ziffern entfernt werden. Von der Startzeit in dieser Ausgabe, `1084798479 = Mo. Mai 17 12:54:39 2004 (GMT)` erhalten Sie.

Geben Sie in der CLI **iplog-status ein**, um diese Ausgabe zu erhalten:

```
"
Log ID:              138343946
IP Address:          xxx.xxx.xxx.xxx
Group:               0
Status:              completed
Start Time:          1084798479512524000
End Time:            1084798510136582000
Bytes Captured:      2833
Packets Captured:    14
"
```

F. Der **"IOException when try to get certificate: java.security.cert.CertificateExpiredException".** Fehlermeldung wird angezeigt. Wie lässt sich dies beheben?

Antwort: Melden Sie sich zur Behebung dieser Fehlermeldung beim AIP-SSM an, und geben Sie den Befehl **tls generate-key** im privilegierten EXEC-Modus aus, wie in diesem Beispiel gezeigt:

```
sensor#tls generate-key
```

Hinweis: Diese Auflösung, bei der der Befehl **tls** generate-key verwendet wird, löst auch das Problem, dass AIP-SSM keine Verbindung zum IME herstellen kann.

F. Die **"IOException: Verbindung verweigert:Verbindung. IME IME-Server reagiert nicht. Bitte prüfen Sie, ob die** Fehlermeldung **ausgeführt wird,** während ich IPS in IME hinzufüge. Wie kann dieses Problem behoben werden?

Antwort: Um diese Fehlermeldung zu beheben, wählen Sie **Systemsteuerung > Admin Tools >**

Services und starten Sie IME Services neu.

F. Die `Meldung Konfig.-Benutzername/Kennwort [IOEXception - connect timed out]` wird angezeigt, wenn ich einen IPS-Sensor zur IME hinzufüge. Wie kann dieses Problem behoben werden?

Antwort: Dies weist auf eine unterbrochene Kommunikation zwischen IME und IPS-Sensor hin. Stellen Sie sicher, dass keine Software vorhanden ist, die das SDEE blockiert.

F. Die `"Fehlerantwort vom IME-Server: Unbekannter Fehler (Protokolldatei im Protokollverzeichnis der Installation überprüfen)" .` Fehlermeldung wird angezeigt. Wie kann dieses Problem behoben werden?

Antwort: Um diese Fehlermeldung zu beheben, überprüfen Sie, ob die richtige IP-Adresse verwendet wird, wenn Sie IPS in IME hinzufügen, und überprüfen Sie auch jede Software-Firewall, die auf dem IME-Computer ausgeführt wird und die Verbindung blockieren kann.

F. Können IDS- oder IPS-Sensoren E-Mail-Warnmeldungen senden?

Antwort: Der IDS-Sensor kann keine E-Mail-Warnmeldungen allein senden. Bei Verwendung mit IDS kann Security Monitor E-Mail-Benachrichtigungen senden, wenn der Sensor eine Ereignisregel auslöst.

Weitere Informationen zur Konfiguration von E-Mail-Benachrichtigungen mit Security Monitor finden Sie unter E-Mail-Benachrichtigungen konfigurieren.

Cisco IPS Manager Express (IME) kann so konfiguriert werden, dass E-Mail-Benachrichtigungen (Warnungen) gesendet werden, wenn Event-Regeln von Cisco IPS-Sensoren ausgelöst werden. Weitere Informationen finden Sie unter IPS 6.X und höher: E-Mail-Benachrichtigungen mit IME-Konfigurationsbeispiel für weitere Informationen.

F. Der `Fehler: Kommunikation mit mainApp (getVersion) nicht möglich. Wenden Sie sich an Ihren Systemadministrator.` wird eine Fehlermeldung angezeigt, wenn ich versuche, eine Verbindung zu meinem Sensor herzustellen. Wie kann dieses Problem behoben werden?

Antwort: Starten Sie den Sensor neu, um dieses Problem zu beheben.

F. Die `Warnung: WARNUNG: Es sind nicht genügend Ressourcen verfügbar, um alle derzeit aktiven benutzerdefinierten Regexes zu kombinieren. Einige Warnmeldungen werden nicht ausgelöst. Erwägen Sie die Einstellung von Signaturen, bis diese Nachricht nicht mehr auftritt.` auf meinem Sensor wird eine Signaturanpassung angezeigt. Wie kann dieses Problem behoben werden?

Antwort: Reifen Sie die Signaturen, die nicht verwendet werden, um dieses Problem zu beheben, und auch die Anzahl der Kundensignaturen mit Regexes sollte reduziert werden. Außerdem wird die Verwendung von * und +Metazeichen bei Regexen nicht empfohlen.

F. Warum treten Latenzprobleme bei Sensoren des Cisco Intrusion Prevention

System (IPS) auf? Wie kann dieses Problem behoben werden?

Antwort: Das Latenzproblem kann aufgrund des assymetrischen Routings auftreten. Versuchen Sie, die Signatur 1330 zu deaktivieren, um dieses Problem zu beheben.

F. Ist es möglich, SSHv1 zu deaktivieren und nur das SSHv2 auf den IPS-Sensoren (Intrusion Prevention System) von Cisco zu aktivieren?

Antwort: Derzeit ist es nicht möglich, SSHv1 zu deaktivieren und nur SSHv2 zu aktivieren. Sowohl SSHv1 als auch SSHv2 sind zusammen aktiviert und können nicht einzeln deaktiviert werden.

F. Der **Fehler: Beim Sensor ist während der Aktualisierung ein Fehler aufgetreten. Sensormeldung = Das Update erfordert 115000 KB in /usr/cids/idsRoot/var, es sind nur 110443 KB verfügbar.** wird angezeigt, wenn ich den Sensor auf Version 4.1(5) aktualisiere. Wie kann dieses Problem behoben werden?

Antwort: Diese Fehlermeldung wird angezeigt, weil der Sensor nicht genügend Speicher hat.

Führen Sie diese Schritte aus, um dieses Problem zu beheben:

1. Melden Sie sich bei einem Dienstkonto an, und werden Sie root
2. Entfernen Sie die folgenden Verzeichnisse, wie unten gezeigt:
   ```
   # rm -rf /usr/cids/idsRoot/var/updates/files/S69
   # rm -rf /usr/cids/idsRoot/var/updates/files/common
   # rm /usr/cids/idsRoot/var/virtualSensor/*
   # rm /usr/cids/idsRoot/var/.tmp/*
   ```
3. Versuchen Sie jetzt, den Sensor zu aktualisieren. Weitere Informationen finden Sie unter Cisco Bug ID CSCsb81288 (nur registrierte Kunden).

F. Ich erhalte die **mainApp[396] cplane/E Error - accept() call return -1** Fehlermeldung im Protokoll auf ASA. Wie kann dieser Fehler behoben werden?

Antwort: Die `mainApp[396] cplane/E Error - accept()`-Fehlermeldung`, die zurückgegeben wurde -1`, weist darauf hin, dass der Webserver die Datei nicht lesen kann, und accept()-Programm ist fehlgeschlagen, wodurch Dateideskriptoren ausgegeben werden, wenn TLS-Verbindungen vorhanden sind. Diese Datei wird jedoch nicht für normales Verhalten benötigt. Es ist harmlos.

F. Wie kann ich die **tls/W errTransport WebSession::sessionTask TLS-Verbindungsausnahme auflösen: unvollständige Handshake**-Fehlermeldung?

Antwort: Diese Fehlermeldung weist darauf hin, dass das Zertifikat für das Modul nicht mehr gültig ist. Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Regeneriert das Zertifikat aus der CLI:Melden Sie sich bei der Befehlszeile des Sensors an.Geben Sie den Befehl **tls generate** ein, und drücken Sie **die Eingabetaste**. Notieren Sie die angezeigten Fingerabdrücke.
2. Ziehen Sie das neue Zertifikat in IME:Öffnen Sie das IME, und suchen Sie den Sensornamen in der Liste auf der Startseite.Klicken Sie mit der rechten Maustaste auf den Sensor, und klicken Sie auf **Bearbeiten**.Wenn Sie den Bildschirm "Gerät bearbeiten" erreichen, klicken

Sie auf **OK**. Überspringen Sie alle Warnmeldungen, dass die Sensorzeit nicht abgerufen werden kann.Sie werden aufgefordert, das neue Sicherheitszertifikat (das soeben erstellte Sicherheitszertifikat) einzugeben. Überprüfen Sie, ob die Fingerabdrücke übereinstimmen, und klicken Sie auf **Ja**.Nach einigen Sekunden sollte der Sensor im Ereignisstatus erneut "Connected" (Verbunden) anzeigen.

F. Wenn ich versuche, mich bei IPS anzumelden, erhalte ich die folgende Fehlermeldung: `errSystemError-ct-sensorAPP.450 reagiert nicht, clientpipe ist fehlgeschlagen.` Wie kann ich diesen Fehler beheben?

Antwort: Um diesen Fehler zu beheben, verwenden Sie den **Befehl reset (Zurücksetzen)**, um das IPS neu zu starten.

F. Die Zeit für AIP-SSM unterscheidet sich von der Zeit für die Cisco Adaptive Security Appliance (ASA). Wie kann dieses Problem behoben werden?

Antwort: Verwenden Sie zur Behebung dieses Problems den NTP-Server, um die Uhrzeit auf der Cisco Adaptive Security Appliance (ASA) und dem AIP-SSM zu synchronisieren.

Weitere Informationen finden Sie unter Konfigurieren von NTP auf IPS-Sensoren.

F. Wie kann ich mehrere virtuelle Sensoren auf AIP-SSM anwenden?

Antwort: Virtuelle Sensoren auf AIP-SSM können nicht pro Schnittstelle angewendet werden, da das AIP-SSM nur über eine Schnittstelle verfügt. Wenn Sie mehrere virtuelle Sensoren erstellen, müssen Sie diese Schnittstelle nur einem virtuellen Sensor zuweisen. Sie müssen keine Schnittstelle für die anderen virtuellen Sensoren festlegen.

Nachdem Sie virtuelle Sensoren erstellt haben, müssen Sie diese mithilfe des Befehls **assigned-ips** einem Sicherheitskontext auf der Adaptive Security Appliance (ASA) zuordnen. Sie können viele Sicherheitskontexte vielen virtuellen Sensoren zuordnen. Weitere Informationen finden Sie im Abschnitt *Zuweisen von virtuellen Sensoren zu Adaptive Security Appliance Contexts* unter Konfigurieren von AIP-SSM.

F. Wie viele virtuelle Sensoren unterstützt AIP-SSM maximal?

Antwort: Es können maximal vier virtuelle Sensoren unterstützt werden.

F. Wenn ich SSH oder IDM verwende, um mich bei IPS anzumelden, ist es möglich, das IPS 4240/IDSM/IDSM2 zu konfigurieren, um administrative Benutzer auf einem RADIUS/TACACS+-Server zu validieren?

Antwort: Mit einem TACACS+-Server ist dies nicht möglich, RADIUS wird jedoch von der IPS 7.0.(4)E4-Version unterstützt. Weitere Informationen finden Sie in den Abschnitten *Neue und geänderte Informationen* und *Einschränkungen und Beschränkungen* der Versionshinweise für das Cisco Intrusion Prevention System 7.0(4)E4. Weitere Informationen finden Sie unter IPS 7.X: Benutzeranmeldeauthentifizierung mit ACS 5.X als RADIUS-Server-Konfigurationsbeispiel für eine Beispielkonfiguration.

F. Welche Auswirkungen hat eine abgelaufene Lizenz auf die IPS-Funktionalität?

Antwort: Die einzige Auswirkung einer abgelaufenen Lizenz auf den Sensor besteht darin, dass die Signatur-Updates angehalten werden.

F. Haben die IPS-Signatur-Updates Auswirkungen auf die Services oder die Netzwerkverbindung?

Antwort: Nein. Die IPS-Signatur-Updates haben keine Auswirkungen auf die Services oder die Netzwerkverbindung.

F. Wie lautet die genaue URL, die ich eingeben muss, damit das IPS-Modul automatisch mit den neuesten Signaturen aktualisiert werden kann?

Antwort: Der Link, der für die automatische Aktualisierung des IPS-Moduls mit der neuesten Signatur erforderlich ist, lautet: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Sie müssen Ihre Cisco Benutzer-ID und Ihr Kennwort verwenden, um die Aktualisierung des IPS-Moduls abzuschließen.

Hinweis: Im 6.x-Train des Codes werden automatische Updates von Cisco.com nicht unterstützt. Sie müssen die Signaturdateien manuell herunterladen und auf den Sensor anwenden. Der 6.x-Code verfügt über eine automatische Aktualisierungsfunktion. Dies ist jedoch nur von einem lokalen Dateiserver möglich, auf den die Signaturdateien auch manuell heruntergeladen werden müssen.

F. Ist der IPS-Sensor anfällig für die X11-Port Forwarding Session Hijack-Schwachstelle?

Antwort: Nein. Sie ist aus folgenden Gründen nicht anfällig:

- Der Sensor verfügt nicht über X11-Bibliotheken. Daher gibt es keine Sitzungen zum Hijack.
- Die X11-Port-Weiterleitung ist in der SSH-Konfiguration nicht aktiviert.
- IPv6 wird nicht in den Sensorkernel kompiliert. Dies ist erforderlich, um die Schwachstelle auszunutzen.

F. Warum zeigt das AIP-SSM keine Protokolle an, wenn die ASA ausreichend Warn- und Angriffsprotokolle anzeigt?

Antwort: Dies liegt daran, dass ASA-Geräte, die sie blockieren, nicht zur doppelten Überprüfung an das IPS weitergeleitet werden. Aus diesem Grund können keine doppelten Protokolle auf ASA und IPS angezeigt werden.

F. Nachdem ein Benutzer den S518-Signatursatz bereitgestellt hat, wird die Fehlermeldung "`invalidValue:Editing string-xl-tcp sig XXXX has NO effect in this version`" angezeigt. Warum?

Antwort: Dies ist die vollständige Fehlermeldung:

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

Dieses Problem tritt auf, weil die String-xl-tcp- oder string-tcp-xl-Engine von der Hardware nicht unterstützt wird. Weitere Informationen finden Sie in den Versionshinweisen zur IPS-Engine E4.

F. Wenn ich die Signaturen auf einem ASA-SSM-10 automatisch mit der Funktion zur automatischen Aktualisierung aktualisiere, erhalte ich die folgende Fehlermeldung: **Es wurde kein installierbares Auto-Update-Paket auf server status=true gefunden.** Wie kann ich dieses Problem beheben?

Antwort: Diese Ausgabe zeigt die vollständige Fehlermeldung an:

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Dieser Fehler wurde generiert, und die Signaturen werden nicht automatisch aktualisiert, da die Signature-Definition-Updates nach S479 das E4-Modul erfordern. Um dies zu beheben, müssen Sie den Sensor manuell auf 7.0(2)E4 aktualisieren.

Hinweis: Der Sensor kann sich nicht automatisch auf E4 aktualisieren, da 7.0(2) und ein Neustart des Sensors erforderlich sind.

F. Die automatische Update-Funktion auf dem IPS 5.0 für NIDS-Modul funktioniert nicht. Wie kann ich dieses Problem beheben?

Antwort: Diese Ausgabe zeigt die vollständige Fehlermeldung an:

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Dieses Problem tritt auf, weil beim FTP-Server ein falscher Verzeichnislistenstil vorliegt. Um dies zu beheben, wechseln Sie zu UNIX-artigen Verzeichnisauflistungen aus den vorhandenen MS-DOS-Verzeichnissen.

Um die Verzeichnislisteneinstellungen zu ändern, wählen Sie **Start** > **Programmdateien** > **Verwaltung**, um den Internet Services Manager zu öffnen. Wechseln Sie dann zur Registerkarte "Home Directory" (Startverzeichnis), und ändern Sie den Verzeichnislistenstil von MS-DOS in UNIX.

F. IPS-4255 erhält die Fehlermeldung SensorApp in TcpRootNode::expireNow() während eines Upgrades fehlschlägt. Wie kann ich dieses Problem beheben?

Antwort: Dieses Problem ist auf den Ausfall der Analyse-Engine zurückzuführen und wird in Cisco Bug ID CSCtb39179 behandelt (nur registrierte Kunden) . Aktualisieren Sie den Sensor auf Version 7.0(4)E4, um dieses Problem zu beheben.

F. Wenn ich versuche, eine Lizenzaktualisierung durchzuführen, nachdem ich eine neue Lizenz erworben habe, meldet das Gerät diesen Fehler: **"Lizenz auf Sensor konnte nicht aktualisiert werden." "errExpiredLicense - Das neue Lizenzablaufdatum ist älter als das aktuelle Lizenzablaufdatum."** Wie kann ich dieses Problem beheben?

Antwort: Dieses Problem tritt auf, wenn die erhaltene Lizenzdatei ungültig ist. Um eine gültige Lizenzdatei zu erhalten, melden Sie sich bei Cisco.com als registrierter Benutzer an, und laden Sie die entsprechende Lizenzdatei herunter. Sobald Sie die gültige Lizenzdatei erhalten haben, installieren Sie sie auf Ihrem Sensor.

Wenn Sie die neue Lizenzdatei installieren und immer noch einen Fehler erhalten, kann es zu einem Problem mit der vorhandenen ungültigen Lizenzdatei kommen. Gehen Sie wie folgt vor, um dieses Problem zu beheben und die vorhandene ungültige Lizenzdatei zu löschen:

1. Melden Sie sich beim Dienstkonto an, indem Sie den Benutzernamen Ihres Dienstkontos eingeben.Wenn Sie kein Dienstkonto haben, öffnen Sie die IPS-Befehlszeile, wechseln Sie in den Konfigurationsmodus, und geben Sie diesen Befehl ein.**Benutzername *Name* privilege service password *password***
   ```
   ciscoasa# session 1
   Opening command session with slot 1.

   Connected to slot 1. Escape character sequence is 'CTRL-^X'.
   login:
   Password:

   IPS#
   IPS#conf t
   IPS(config)# username name privilege service password password
   ```
2. Wenn Sie sich bei Ihrem Dienstkonto angemeldet haben, geben Sie den Befehl **su** ein, um zum Stammverzeichnis zu wechseln (mit dem gleichen Kennwort wie das Dienstkonto).
3. Löschen Sie die Dateien im Verzeichnis /usr/cids/idsRoot/shared/.**Hinweis:** Löschen Sie nicht die Datei host.conf.Geben Sie den Befehl **cd /usr/cids/idsRoot/shared/** ein, um zum freigegebenen Verzeichnis zu wechseln.Geben Sie den Befehl **ls** ein, um die Dateien im Verzeichnis anzuzeigen.Geben Sie den Befehl **rm *file_name ein*, um die Dateien zu entfernen.Hinweis:** Löschen Sie nicht die Datei host.conf.
4. Geben Sie den Befehl **/etc/init.d/cids restart** ein, um den Sensor neu zu starten.
5. Installieren Sie die neue Lizenz.

Für dieses Verhalten wurde ein Fehler von Cisco gemeldet. Weitere Informationen finden Sie unter CSCtg76339 (nur registrierte Kunden).

F. Was tut die **errorMessage: IPlog 1712041197 wurde aufgrund fehlender Dateihandles früh beendet. name=ErrLimitExceeded** Fehlermeldung bedeuten? Wie kann ich dieses Problem beheben?

Antwort: Dieser Fehler wird durch eine übermäßige Anzahl von Paketen bei der IP-Protokollierung verursacht. Deaktivieren Sie die IP-Protokollierungsfunktion, um dieses Problem zu beheben. Die IP-Protokollierung ist nur für die Fehlerbehebung vorgesehen. Cisco empfiehlt, dass Sie es nicht

für alle Signaturen aktivieren.

F. Ich erhalte diesen Fehler, wenn ich den Sensor von s550 auf s551 aktualisiere: `Die aktuelle Konfiguration für die Komponente "signaturdefinition" und die Instanz "sig0"kann nicht analysiert werden.` Wie kann ich dieses Problem beheben?

Antwort: Die Änderung der Signatur 23899.0 verursacht dieses Problem. Weitere Informationen finden Sie unter Cisco Bug ID CSCtn84552 (nur registrierte Kunden).

F. Ich erhalte diesen Fehler auf dem Sensor: `Fehler: autoUpdate hat erfolgreich ein Paket vom Cisco.com Locator-Dienst ausgewählt. Der Paketdownload ist jedoch fehlgeschlagen: Die HTTP-Antwort konnte nicht empfangen werden.` Wie kann ich dieses Problem beheben?

Antwort: Überprüfen Sie, ob URL-Filterung, Content-Filterung oder ein Proxy-Server vorhanden sind, der die automatische Aktualisierung blockiert. Stellen Sie sicher, dass autoUpdate nicht blockiert wird, und überprüfen Sie, ob die angegebenen Benutzeranmeldeinformationen korrekt sind.

F. Ich erhalte diese XML-Fehlermeldung auf dem IPS-Sensor, der mit Version 6.2(3)E4 ausgeführt wird: `errorMessage: IPS-Software versuchte, ungültige XML-Daten für (Token) zu schreiben. Ungültige XML-Zeichen wurden durch '*'ersetzt.` Wie kann ich dieses Problem beheben?

Antwort: Dieses Verhalten wurde durch die Cisco Bug ID CSCsq50873 behoben (nur registrierte Kunden). Dies ist ein kosmetisches Problem und verursacht keinen betrieblichen Mehraufwand, außer der übermäßigen Anzahl der empfangenen Protokolle. Eine vorübergehende Lösung besteht darin, die NTP-bezogene Konfiguration auf dem Sensor zu entfernen. Für eine permanente Lösung, aktualisieren Sie auf eine Version, in der dieser Fehler behoben ist.

F. Warum stellt die IME-Workstation konstante Verbindungen zu verwalteten Servern her, obwohl der Client geschlossen wurde?

Antwort: IME fungiert als zwei Windows-Dienste und als GUI-Client. Wenn der Client geschlossen wird, werden die beiden Windows-Dienste (Cisco IPS Manager Express und MySQL-IME) weiterhin ausgeführt, Ereignisse von den verwalteten Sensoren erfassen und in der lokalen MySQL-Datenbank speichern. Dadurch können Verlaufsberichte erstellt werden.

Der IME-Client sollte ein einziges SDEE-Abonnement für den verwalteten Sensor öffnen und dieses Abonnement für die nachfolgenden Aktivitäten zum Abruf von Ereignissen wiederverwenden. Das erwartete Verhalten ist die konstante Verbindung von der IME-Workstation zu den verwalteten Sensoren.

F. Kann das AIP-SSM-Modul als SPAN-Ziel verwendet werden?

Antwort: Nein. Das AIP-SSM-Modul kann nicht als SPAN-Ziel verwendet werden, da es nur zur Überwachung des Datenverkehrs verwendet wird, der durch die ASA-Schnittstelle fließt.

F. Warum wird eine hohe CPU-Auslastung beobachtet, nachdem das IPS auf die E3-Engine aktualisiert wurde?

Antwort: Bei E3-Engine-Updates verwendet das IPS einen anderen Algorithmus zur Verwaltung der Leerlaufzeit und verbringt mehr Zeit mit dem Polling von Paketen, um die Latenz zu verringern. Diese verstärkte Überprüfung führt zu einer entsprechenden Erhöhung der CPU-Auslastung. Die korrekte Methode zur Messung der CPU in E3 ist nicht die CPU-Auslastung, sondern der **Paketlastungsprozentsatz**, der die korrekte CPU-Auslastung anzeigt.

F. Warum leuchtet die Status-LED bei meiner IPS-Appliance periodisch rot?

Antwort: Dies kann durch ein falsches Zertifikat auf der Remote-Managementkonsole geschehen, das Software wie CS-MARS, CSM, IEV, VMS-IDS/IPSMC usw. ausführt. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Wenden Sie das TLS-Zertifikat des Sensors auf der Remote-Managementstation an.
2. Konfigurieren Sie einen gültigen DNS-Server.

F. Wie kann das IPS verhindern, dass der HTTP-Datenverkehr verzögert wird, während die Schnittstellen durchlaufen werden?

Antwort: Wenn Sie den Sensor so konfigurieren, dass er im asymmetrischen Modus funktioniert, wird das Problem behoben. Führen Sie die folgenden Schritte aus, um den Sensor in den Schutz des asymmetrischen Modus zu versetzen:

1. Gehen Sie zu **Konfiguration > Richtlinien > IPS-Richtlinien**.
2. Doppelklicken Sie auf **Virtueller Sensor**.
3. Gehen Sie zu **Erweiterte Optionen**.
4. Wählen Sie unter Normalisierungsmodus die Option **Schutz im asymmetrischen Modus aus**.
5. Klicken Sie auf **OK**.
6. Starten Sie die Einheit neu, damit die Änderungen wirksam werden.

Zugehörige Informationen

- Support-Seite für das Cisco Secure Intrusion Prevention System
- Fehlerbehebung für AIP-SSM
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- Technischer Support und Dokumentation - Cisco Systems