Technische Hinweise zu häufig gestellten Fragen zum Remote-Zugriff auf Cisco ESA/WSA/SMA

Inhalt

Einführung

Dieses Dokument enthält Antworten auf häufig gestellte Fragen zur Verwendung des Remote-Zugriffs durch den technischen Support von Cisco auf Cisco Content Security Appliances. Dazu gehören die Cisco E-Mail Security Appliance (ESA), die Cisco Web Security Appliance (WSA) und die Cisco Security Management Appliance (SMA).

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Cisco Content Security Appliances, auf denen eine beliebige Version von AsyncOS ausgeführt wird.

Was ist Remote-Zugriff?

Der Remote-Zugriff ist eine Secure Shell (SSH)-Verbindung, die von einer Cisco Content Security-Appliance zu einem sicheren Host bei Cisco aktiviert wird. Nur Cisco Customer Assistance kann auf die Appliance zugreifen, sobald eine Remotesitzung aktiviert wurde. Der Remote-Zugriff ermöglicht dem Cisco Kundensupport die Analyse einer Appliance. Der Support greift über einen

SSH-Tunnel zwischen der Appliance und dem Upgrade.ironport.com-Server auf die Appliance zu.

Funktionsweise von Remote-Zugriff

Wenn eine Remotezugriffsverbindung initiiert wird, öffnet die Appliance einen sicheren, zufälligen, hochSource-Port über eine SSH-Verbindung auf der Appliance mit dem konfigurierten/ausgewählten Port eines der folgenden Cisco Content Security-Server:

IP-Adresse	Hostname	Verwenden
63 251 108 107	Upgrades.ironport.com	Alle Content Security Appliances
63 251 108 107	c.tunnels.ironport.com	Appliances der C-Serie (ESA)
63 251 108 107	x.tunnels.ironport.com	Appliances der X-Serie (ESA)
63 251 108 107	m.tunnels.ironport.com	Appliances der M-Serie (SMA)
63 251 108 107	s.tunnels.ironport.com	Appliances der S-Serie (WSA)

Beachten Sie, dass möglicherweise eine Kunden-Firewall konfiguriert werden muss, um ausgehende Verbindungen zu einem der oben aufgeführten Server zuzulassen. Wenn die SMTP-Protokollüberprüfung für Ihre Firewall aktiviert ist, wird der Tunnel nicht eingerichtet. Folgende Ports werden von Cisco Verbindungen von der Appliance für den Remote-Zugriff akzeptiert:

- 22
- 25 (Standard)
- 53
- 80
- 443
- 4766

Die Remote-Zugriffsverbindung wird mit einem Hostnamen und nicht mit einer hartcodierten IP-Adresse hergestellt. Dies erfordert, dass der Domain Name Server (DNS) auf der Appliance konfiguriert wird, um die ausgehende Verbindung herzustellen.

In einem Kundennetzwerk blockieren einige protokollsensitive Netzwerkgeräte diese Verbindung aufgrund der Protokoll-/Port-Diskrepanz. Einige Simple Mail Transport Protocol (SMTP)-fähige Geräte unterbrechen möglicherweise auch die Verbindung. In Fällen, in denen protokollsensitive Geräte oder ausgehende Verbindungen blockiert sind, kann die Verwendung eines anderen Ports als des Standards (25) erforderlich sein. Der Zugriff auf das Remote-Ende des Tunnels ist auf den Cisco Kundensupport beschränkt. Bitte überprüfen Sie Ihre Firewall/Ihr Netzwerk auf ausgehende Verbindungen, wenn Sie versuchen, Remotezugriffsverbindungen für Ihre Appliance herzustellen oder eine Fehlerbehebung vorzunehmen.

> **Hinweis**: Wenn ein Cisco Customer Support Engineer über Remote-Zugriff mit der Appliance verbunden ist, wird die Systemaufforderung auf der Appliance *(SERVICE)* angezeigt.

So aktivieren Sie den Remote-Zugriff

> **Hinweis**: Anweisungen zum Aktivieren des Remote-Zugriffs für Mitarbeiter des technischen Supports von Cisco finden Sie im Benutzerhandbuch Ihrer Appliance und in der Version von AsyncOS.

Hinweis: Anhänge, die per E-Mail an attach@cisco.com gesendet werden, sind möglicherweise bei der Übertragung nicht sicher. Support Case Manager ist die bevorzugte sichere Option von Cisco, um Informationen auf Ihr Ticket hochzuladen. Weitere Informationen zu den Sicherheits- und Größenbeschränkungen anderer Datei-Upload-Optionen finden Sie unter: Uploads von Kundendateien an das Cisco Technical Assistance Center

Identifizieren Sie einen Port, der über das Internet erreichbar ist. Der Standardwert ist Port 25, der in den meisten Umgebungen verwendet wird, da das System auch allgemeinen Zugriff über diesen Port benötigt, um E-Mail-Nachrichten zu senden. Verbindungen über diesen Port sind in den meisten Firewall-Konfigurationen zulässig.

CLI

Gehen Sie wie folgt vor, um als Administrator-Benutzer über die CLI eine Remote-Zugriffsverbindung herzustellen:

1. Geben Sie den Befehl **techsupport ein.**
2. **TUNNEL** auswählen
3. Auswählen, um eine zufällige Seed-Zeichenfolge zu generieren oder *einzugeben*
4. Geben Sie die Portnummer für die Verbindung an.
5. Antwort **"Y"** zur Aktivierung des Dienstzugriffs

Der Remote-Zugriff wird zu diesem Zeitpunkt aktiviert. Die Appliance arbeitet nun an der Herstellung einer sicheren Verbindung mit dem Secure Bastion Host bei Cisco. Geben Sie sowohl die Seriennummer der Appliance als auch die Zeichenfolge an, die für den TAC-Techniker generiert wird, der Ihr Ticket unterstützt.

Benutzeroberfläche

Gehen Sie wie folgt vor, um als Administrator-Benutzer über die GUI eine Remote-Zugriffsverbindung herzustellen:

1. Navigieren Sie zu **Hilfe und Support > Remote Access** (für ESA, SMA), **Support and Help > Remote Access** (für WSA).
2. Klicken Sie auf **Aktivieren.**
3. Wählen Sie die Methode für die Seed-Zeichenfolge aus
4. Aktivieren Sie das Kontrollkästchen *Verbindung über sicheren Tunnel initiieren*, und geben Sie die Anschlussnummer für die Verbindung an.
5. Klicken Sie auf **Senden**

Der Remote-Zugriff wird zu diesem Zeitpunkt aktiviert. Die Appliance arbeitet nun an der Herstellung einer sicheren Verbindung mit dem Secure Bastion Host bei Cisco. Geben Sie sowohl die Seriennummer der Appliance als auch die Zeichenfolge an, die für den TAC-Techniker generiert wird, der Ihr Ticket unterstützt.

Deaktivieren des Remote-Zugriffs

CLI

1. Geben Sie den Befehl **techsupport ein.**
2. Wählen Sie **DISABLE**
3. Beantworten Sie **"Y"**, wenn Sie gefragt werden, ob Sie den Servicezugriff wirklich deaktivieren möchten.

Benutzeroberfläche

1. Navigieren Sie zu **Hilfe und Support > Remote Access** (für ESA, SMA), **Support and Help > Remote Access** (für WSA).
2. Klicken Sie auf **Deaktivieren.**
3. In der GUI-Ausgabe wird "Success — Remote Access has been disabled" angezeigt.

Testen der Remote-Zugriffsverbindung

Verwenden Sie dieses Beispiel, um einen ersten Test für die Verbindung zwischen Ihrer Appliance und Cisco durchzuführen:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

Die Verbindung kann für jeden der oben aufgeführten Ports getestet werden: 22, 25, 53, 80, 443 oder 4766. Wenn die Verbindung fehlschlägt, müssen Sie möglicherweise eine Paketerfassung durchführen, um festzustellen, wo die Verbindung von Ihrer Appliance/Ihrem Netzwerk ausfällt.

Warum funktioniert der Remote-Zugriff für das SMA nicht?

Der Remote-Zugriff kann bei einer SMA nicht aktiviert werden, wenn die SMA im lokalen Netzwerk ohne direkten Internetzugang platziert wird. In diesem Fall kann der Remote-Zugriff auf einer ESA oder WSA aktiviert werden, und der SSH-Zugriff kann auf der SMA aktiviert werden. Auf diese Weise kann der Cisco Support zuerst über Remote-Zugriff eine Verbindung zur ESA/WSA herstellen und dann über SSH von der ESA/WSA zur SMA. Dies erfordert eine Verbindung zwischen der ESA/WSA und der SMA an Port 22.

> **Hinweis**: Anweisungen zum Aktivieren des Remote-Zugriffs auf Appliances ohne direkte Internetverbindung finden Sie im Benutzerhandbuch Ihrer Appliance und in der Version von AsyncOS.

CLI

Gehen Sie wie folgt vor, um als Administrator-Benutzer über die CLI eine Remote-Zugriffsverbindung herzustellen:

1. Geben Sie den Befehl **techsupport ein.**
2. **SSHACCESS** auswählen

3. Auswählen, um eine zufällige Seed-Zeichenfolge zu generieren oder *einzugeben*
4. Antwort "**Y**" zur Aktivierung des Dienstzugriffs

Der Remote-Zugriff wird zu diesem Zeitpunkt aktiviert. Die CLI-Ausgabe zeigt die Seed-Zeichenfolge an. Bitte geben Sie diese an den Cisco Customer Support Engineer weiter. Die CLI-Ausgabe zeigt auch den Verbindungsstatus und Details zum Remote-Zugriff an, einschließlich der Seriennummer der Einheit. Bitte geben Sie diese Seriennummer dem Kundensupporttechniker an.

Benutzeroberfläche

Gehen Sie wie folgt vor, um als Administrator-Benutzer über die GUI eine Remote-Zugriffsverbindung herzustellen:

1. Navigieren Sie zu **Hilfe und Support > Remote Access** (für ESA, SMA), **Support and Help > Remote Access** (für WSA).
2. Klicken Sie auf **Aktivieren.**
3. Wählen Sie die Methode für die Seed-Zeichenfolge aus
4. Aktivieren Sie NICHT das Kontrollkästchen *Verbindung über sicheren Tunnel initiieren*.
5. Klicken Sie auf **Senden**

Der Remote-Zugriff wird zu diesem Zeitpunkt aktiviert. Die GUI-Ausgabe zeigt eine Erfolgsmeldung und die Seed-Zeichenfolge der Appliance an. Bitte geben Sie diese an den Cisco Customer Support Engineer weiter. Die GUI-Ausgabe zeigt auch den Verbindungsstatus und die Details zum Remote-Zugriff an, einschließlich der Seriennummer der Einheit. Bitte geben Sie diese Seriennummer dem Kundensupporttechniker an.

Deaktivieren des Remote-Zugriffs bei Aktivierung von SSHACCESS

Die Deaktivierung des Remote-Zugriffs für SSHACCESS entspricht den oben beschriebenen Schritten.

Fehlerbehebung

Wenn die Appliance nicht in der Lage ist, den Remote-Zugriff zu aktivieren und über einen der aufgeführten Ports eine Verbindung zu upgrade.ironport.com herzustellen, müssen Sie eine Paketerfassung direkt von der Appliance aus ausführen, um zu überprüfen, was dazu führt, dass die ausgehende Verbindung fehlschlägt.

> **Hinweis**: Anweisungen zum "Ausführen einer Paketerfassung" finden Sie im Benutzerhandbuch Ihrer Appliance und in der Version von AsyncOS.

Der Cisco Customer Support Engineer kann beantragen, dass die .pcap-Datei zur Überprüfung und Unterstützung bei der Fehlerbehebung bereitgestellt wird.

Zugehörige Informationen

- Häufig gestellte Fragen zur ESA: Wie hoch ist der administrative Zugang, der über die ESA möglich ist?

- Produkt-Support für Cisco Email Security Appliance
- Cisco Web Security-Produktsupport
- Produkt-Support für die Cisco Content Security Management Appliance
- Technischer Support und Dokumentation - Cisco Systems