Technische opmerking over FAQ voor externe toegang tot Cisco ESA/WSA/SMA

Inhoud

Inleiding

Dit document bevat antwoorden op vaak gestelde vragen over het gebruik van externe toegang door Cisco Technical Support op Cisco Content Security Appliance. Dit omvat de Cisco e-mail security applicatie (ESA), Cisco web security applicatie (WSA) en Cisco Security Management applicatie (SMA).

Voorwaarden

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Content Security Appliance die elke versie van AsyncOS uitvoert.

Wat is toegang op afstand?

Externe toegang is een Secure Shell (SSH)-verbinding die via een Cisco Content Security Appliance aan een beveiligde host bij Cisco wordt ingeschakeld. Alleen Cisco Customer Assistance kan het apparaat benaderen nadat er een externe sessie is geactiveerd. Externe toegang stelt Cisco Customer Support in staat een apparaat te analyseren. Ondersteuning heeft

toegang tot het apparaat via een SSH-tunnel die door deze procedure wordt gecreëerd tussen het apparaat en de server upgrades.ironport.com.

Hoe toegang op afstand werkt

Wanneer een externe toegangsverbinding wordt gestart, opent het apparaat een beveiligde, willekeurige, hoge-bronpoort via een SSH-verbinding op het apparaat naar de geconfigureerde/geselecteerde poort van een van de volgende Cisco Content Security-servers:

IP-adres	schuilnaam	Gebruik
63.251.108.107	upgrades.ironport.com	Alle content security applicaties
63.251.108.107	c.tunnels.ironport.com	C-Series-apparaten (ESA's)
63.251.108.107	x.tunnels.ironport.com	X-Series-apparaten (ESA)
63.251.108.107	m.tunnels.ironport.com	M-Series apparaten (SMA)
63.251.108.107	s.tunnels.ironport.com	S-Series apparaten (WSA)

Het is belangrijk om op te merken dat een firewall van een klant moet worden geconfigureerd om uitgaande verbindingen naar een van de bovengenoemde servers mogelijk te maken. Als uw firewall TCP inspectie heeft toegelaten, zal de tunnel niet opstellen. Poorten die Cisco verbindingen van het apparaat voor de externe toegang zal accepteren zijn:

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

De externe toegangsverbinding wordt gemaakt met een host-naam en niet met een gecodeerd IP-adres. Hiervoor moet Domain Name Server (DNS) op het apparaat zijn ingesteld om de uitgaande verbinding te kunnen opzetten.

Op een klantnetwerk kunnen sommige protocol-bewuste netwerkapparaten deze verbinding blokkeren vanwege een protocol/poort-mismatch. Sommige Simple Mail Transport Protocol (MTP)-bewuste apparaten kunnen de verbinding ook onderbreken. In gevallen waar er protocol-bewuste apparaten of uitgaande verbindingen zijn geblokkeerd, kan het gebruik van een poort anders dan de standaard (25) vereist zijn. Toegang tot het externe einde van de tunnel is alleen beperkt tot Cisco Customer Support. Zorg ervoor dat u uw firewall/netwerk opnieuw bekijkt voor uitgaande verbindingen wanneer u probeert om externe toegangsverbindingen voor uw apparaat op te zetten of op te lossen.

> Opmerking: Wanneer een Cisco Customer Support Engineer-eigenaar via externe toegang op het apparaat is aangesloten, wordt de systeemmelding in het apparaat *(SERVICE)* weergegeven.

Toegang op afstand inschakelen

> Opmerking: Zorg ervoor dat u de gebruikershandleiding van uw apparaat en de versie van AsyncOS raadpleegt voor instructies over "Externe toegang voor Cisco Technical Support Personeel".

> Opmerking: Attachments die per e-mail naar attach@cisco.com worden verstuurd, zijn mogelijk niet veilig op doorreis. Support Case Manager is de door Cisco aanbevolen beveiligde optie om informatie naar uw case te uploaden. U kunt als volgt meer informatie krijgen over de beveiliging en de groottebeperkingen van andere opties voor het uploaden van bestanden: Uploaden van klantbestanden naar Cisco Technical Assistance Center

Identificeer een haven die van het internet kan worden bereikt. Het standaard is port 25, dat in de meeste omgevingen zal werken omdat het systeem ook algemene toegang over die poort vereist om e-mailberichten te verzenden. Aansluitingen via deze poort zijn toegestaan in de meeste firewallconfiguraties.

CLI

Voltooi de volgende stappen om een externe toegangsverbinding via de CLI, als een beheerder, op te zetten:

1. Typ de opdracht **technische ondersteuning**
2. **TUNNEL** kiezen
3. Kies om een willekeurige zaadstring te genereren of *in te voeren*
4. Specificeer het poortnummer voor de verbinding
5. Beantwoord **"Y"** om toegang tot de service mogelijk te maken

Externe toegang wordt momenteel ingeschakeld. Het apparaat werkt nu om de beveiligde verbinding naar de beveiligde bastion-host in Cisco tot stand te brengen. Geef zowel het serienummer van het apparaat als de startkabel op die is gegenereerd naar de TAC Engineer die uw case ondersteunt.

GUI

Voltooi de volgende stappen om een externe toegangsverbinding via de GUI, als een beheerder, op te zetten:

1. Navigeren in om **te helpen en te ondersteunen > Externe Toegang** (voor ESA, SMA), **Ondersteuning en Help > Externe Toegang** (voor WSA)
2. Klik op **Inschakelen**
3. Kies de methode voor de zaadstring
4. Zorg ervoor dat u de *verbinding van het Initiate via veilige* tunnelcontrole controleert en het poortnummer voor verbinding specificeert
5. Klik op **Inzenden**

Externe toegang wordt momenteel ingeschakeld. Het apparaat werkt nu om de beveiligde verbinding naar de beveiligde bastion-host in Cisco tot stand te brengen. Geef zowel het serienummer van het apparaat als de startkabel op die is gegenereerd naar de TAC Engineer die uw case ondersteunt.

Toegang op afstand uitschakelen

CLI

1. Typ de opdracht **technische ondersteuning**

2. **UITSCHAKELEN** kiezen
3. Antwoord **"Y"** indien wordt gevraagd "Weet u zeker dat u de toegang tot de service wilt uitschakelen?"

GUI

1. Navigeer in om **te helpen en te ondersteunen > Externe Toegang** (voor ESA, SMA), **Ondersteuning en Help > Externe Toegang** (voor WSA).
2. Klik op **Uitschakelen**
3. De GUI-uitvoer toont "Succes — Externe Toegang is uitgeschakeld"

Hoe de connectiviteit op afstand te testen

Gebruik dit voorbeeld om een eerste test uit te voeren voor de aansluitingen van uw apparaat naar Cisco:

```
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
```

De connectiviteit kan worden getest voor een van de bovengenoemde poorten: 22, 25, 53, 80, 443 of 4766. Als de connectiviteit niet goed werkt, kunt u een pakketvastlegging moeten uitvoeren om te zien waar de verbinding niet bij uw apparaat/netwerk werkt.

Waarom werkt de toegang op afstand niet aan de SMA?

Externe toegang is mogelijk niet mogelijk op een SMA indien de SMA in het lokale netwerk is geplaatst zonder directe toegang tot internet. Bijvoorbeeld, de toegang op afstand kan op een ESA of WSA worden geactiveerd, en SSH toegang kan op de SMA worden geactiveerd. Hiermee kan Cisco-ondersteuning eerst worden aangesloten via externe toegang tot de ESA/WSA, en vervolgens van de ESA/WSA naar de SMA via SSH. Dit vereist connectiviteit tussen de ESA/WSA en de SMA op haven 22.

> Opmerking: Zorg ervoor dat u de gebruikershandleiding van uw apparaat en de versie van AsyncOS raadpleegt voor instructies over "Externe toegang tot applicaties zonder directe internetverbinding inschakelen".

CLI

Voltooi de volgende stappen om een externe toegangsverbinding via de CLI, als een beheerder, op te zetten:

1. Typ de opdracht **technische ondersteuning**
2. **SSHACCESS** kiezen
3. Kies om een willekeurige zaadstring te genereren of *in te voeren*

4. Beantwoord "Y" om toegang tot de service mogelijk te maken

Externe toegang wordt momenteel ingeschakeld. De CLI uitvoer zal de zaadstring tonen. Verstrek dit aan de Cisco Customer Support Engineer. De CLI-uitvoer geeft ook de verbindingsstatus en de gegevens over de toegang op afstand weer, inclusief het serienummer van het apparaat. Geef dit serienummer op aan de Customer Support Engineer.

GUI

Voltooi de volgende stappen om een externe toegangsverbinding via de GUI, als een beheerder, op te zetten:

1. Navigeren in om **te helpen en te ondersteunen > Externe Toegang** (voor ESA, SMA), **Ondersteuning en Help > Externe Toegang** (voor WSA)
2. Klik op **Inschakelen**
3. Kies de methode voor de zaadstring
4. Controleer NIET de *verbinding initiëren via een* selectieteken *voor beveiligde tunnelverbindingen*
5. Klik op **Inzenden**

Externe toegang wordt momenteel ingeschakeld. De GUI-uitvoer geeft u een succesbericht en de startkabel van het apparaat weer. Verstrek dit aan de Cisco Customer Support Engineer. De GUI-uitvoer toont ook de verbindingsstatus en de toegangsgegevens op afstand, inclusief het serienummer van het apparaat. Geef dit serienummer op aan de Customer Support Engineer.

Hoe externe toegang uit te schakelen wanneer dit voor SSHACCESS is ingeschakeld

De toegang op afstand uitschakelen voor SSHACCESS is dezelfde stappen als hierboven zijn beschreven.

Probleemoplossing

Als het apparaat geen toegang op afstand kan inschakelen en geen verbinding met upgrades.ironport.com kan maken via een van de genoemde poorten, dient u een pakketvastlegging direct van het apparaat uit te voeren om te bekijken wat de uitgaande verbinding veroorzaakt.

> Opmerking: Controleer de gebruikershandleiding van uw apparaat en de versie van AsyncOS voor informatie over "Actie bij een pakketvastlegging".

De Cisco Customer Support Engineer kan vragen om het .pcap-bestand te hebben geleverd om de probleemoplossing te bekijken en te ondersteunen.

Gerelateerde informatie

- ESA FAQ: Wat zijn de niveaus van administratieve toegang voor de ESA?
- Cisco e-mail security productondersteuning
- Cisco Web Security productondersteuning

- Cisco Content Security Management-applicatie - productondersteuning
- Technische ondersteuning en documentatie – Cisco Systems