IPsec über TCP schlägt fehl, wenn Datenverkehr über ASA fließt

Inhalt

[Einführung](#)
[Bevor Sie beginnen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Problem](#)
[Lösung](#)
[Zugehörige Informationen](#)

Einführung

Cisco VPN-Clients, die über IPsec über TCP eine Verbindung zu einem VPN-Headend herstellen, können zwar eine Verbindung zum Headend herstellen, die Verbindung schlägt jedoch nach einiger Zeit fehl. In diesem Dokument wird beschrieben, wie Sie über UDP oder systemeigene ESP-IPsec-Kapselung auf IPsec umstellen, um das Problem zu beheben.

Bevor Sie beginnen

Anforderungen

Um diesem spezifischen Problem zu begegnen, müssen Cisco VPN-Clients so konfiguriert sein, dass sie über IPsec über TCP eine Verbindung zu einem VPN-Headend-Gerät herstellen. In den meisten Fällen konfigurieren Netzwerkadministratoren die ASA so, dass sie Cisco VPN Client-Verbindungen über TCP Port 10000 akzeptiert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco VPN Client.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Problem

Wenn der VPN-Client für IPsec over TCP (cTCP) konfiguriert ist, reagiert die VPN-Clientsoftware nicht, wenn ein doppeltes TCP-ACK empfangen wird, das den VPN-Client zur erneuten Datenübertragung auffordert. Ein doppeltes ACK kann generiert werden, wenn irgendwo zwischen dem VPN-Client und dem ASA-Headend ein Paketverlust auftritt. Der zeitweilige Paketverlust ist eine ziemlich häufige Realität im Internet. Da die VPN-Endpunkte jedoch nicht das TCP-Protokoll verwenden (erinnern Sie sich, dass sie cTCP verwenden), übertragen die Endpunkte weiter und die Verbindung wird fortgesetzt.

In diesem Szenario tritt ein Problem auf, wenn ein anderes Gerät vorhanden ist, z. B. eine Firewall, die die TCP-Verbindung zustandsbezogen verfolgt. Da das cTCP-Protokoll einen TCP-Client nicht vollständig implementiert und doppelte ACKs des Servers keine Antwort erhalten, kann dies dazu führen, dass andere Geräte in der Verbindung mit diesem Netzwerk-Stream den TCP-Datenverkehr verwerfen. Der Paketverlust muss im Netzwerk auftreten, sodass TCP-Segmente fehlen, was das Problem auslöst.

Dies ist kein Fehler, sondern eine Nebenwirkung von Paketverlusten im Netzwerk und der Tatsache, dass cTCP kein echtes TCP ist. Das cTCP versucht, das TCP-Protokoll zu emulieren, indem es die IPsec-Pakete in einen TCP-Header einbindet. Dies ist jedoch der Umfang des Protokolls.

Dieses Problem tritt in der Regel dann auf, wenn Netzwerkadministratoren eine ASA mit einem IPS implementieren oder eine Art von Anwendungsinspektion auf der ASA durchführen, die dazu führt, dass die Firewall als vollständiger TCP-Proxy der Verbindung fungiert. Bei Paketverlusten sucht die ASA die fehlenden Daten im Auftrag des cTCP-Servers oder -Clients, aber der VPN-Client reagiert niemals. Da die ASA die erwarteten Daten nie erhält, kann die Kommunikation nicht fortgesetzt werden. Die Verbindung schlägt daher fehl.

Lösung

Um dieses Problem zu beheben, führen Sie eine der folgenden Aktionen aus:

- Umschalten von IPsec über TCP auf IPsec über UDP oder native Kapselung mit dem ESP-Protokoll.
- Wechseln Sie zum AnyConnect-Client für die VPN-Terminierung, der einen vollständig implementierten TCP-Protokoll-Stack verwendet.
- Konfigurieren Sie die ASA so, dass die tcp-state-bypass für diese spezifischen IPsec-/TCP-Datenflüsse angewendet werden. Dadurch werden im Wesentlichen alle Sicherheitsüberprüfungen für Verbindungen deaktiviert, die mit der Richtlinie "tcp-state-bypass" übereinstimmen. Die Verbindungen können jedoch funktionieren, bis eine andere Auflösung aus dieser Liste implementiert werden kann. Weitere Informationen finden Sie unter Richtlinien und Einschränkungen für die Umgehung des TCP-Zustands.
- Identifizieren Sie die Quelle des Paketverlusts, und ergreifen Sie Korrekturmaßnahmen, um zu verhindern, dass IPsec-/TCP-Pakete im Netzwerk verfallen. Dies ist in der Regel unmöglich oder extrem schwierig, da der Auslöser für das Problem in der Regel ein Paketverlust im Internet ist, der nicht verhindert werden kann.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems