Wie geht die Cisco Web Security Appliance (WSA) mit Skype-Datenverkehr um?

Inhalt

Frage:

Wie geht die Cisco Web Security Appliance (WSA) mit Skype-Datenverkehr um?

Umgebung: Cisco WSA, Skype

Skype ist ein proprietäres VoIP-Netzwerk. Skype agiert hauptsächlich als Peer-to-Peer-Programm und kommuniziert daher nicht direkt mit einem zentralen Server, um zu funktionieren. Skype kann besonders schwer zu blockieren sein, da es auf viele verschiedene Arten versucht, eine Verbindung herzustellen.

Skype stellt eine Verbindung in der folgenden Reihenfolge her:

1. Leiten Sie UDP-Pakete mithilfe von zufälligen Portnummern an andere Peers weiter.
2. Verweisen Sie TCP-Pakete mithilfe von zufälligen Portnummern an andere Peers.
3. Vermittlung von TCP-Paketen an andere Peers über Port 80 und/oder Port 443
4. Getunnelte Pakete über einen Webproxy mit HTTP CONNECT zu Port 443

Bei Bereitstellung in einer expliziten Proxy-Umgebung werden die Methoden 1-3 niemals an die Cisco WSA gesendet. Um Skype zu blockieren, muss es zunächst von einem anderen Standort im Netzwerk blockiert werden. Skype-Schritte 1-3 können wie folgt blockiert werden:

- Firewall: NBAR verwenden, um Skype Version 1 zu blockieren. Weitere Informationen finden Sie unter http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Cisco IPS (ASA): Die Cisco ASA kann Skype potenziell über Signaturen erkennen und blockieren.

Wenn Skype wieder auf die Verwendung eines expliziten Proxys zurückgreift, stellt Skype in der HTTP CONNECT-Anfrage absichtlich keine Clientdetails bereit (auch keine Zeichenfolge von User-Agent). Dies erschwert die Unterscheidung zwischen Skype und einer gültigen CONNECT-Anfrage. Skype wird immer mit Port 443 verbunden, und die Zieladresse ist immer eine IP-Adresse.

Beispiel:

CONNECT 10.129.88.111:443 HTTP/1.0
Proxy-Verbindung: Keepalive

Die folgende Zugriffsrichtlinie blockiert alle CONNECT-Anfragen über die WSA, die mit IP-

Adressen und Port 443 übereinstimmen. Dies entspricht dem gesamten Skype-Datenverkehr. Allerdings werden auch Nicht-Skype-Programme, die versuchen, eine Verbindung zu einer IP-Adresse an Port 443 herzustellen, blockiert.

Blockieren von Skype - Explizite Umgebung mit deaktiviertem HTTPS-Proxy

Erstellen Sie eine benutzerdefinierte URL-Kategorie, um den IP- und Port-443-Datenverkehr abzugleichen:

1. Navigieren Sie zu "Sicherheitsmanager" -> "Benutzerdefinierte URL-Kategorien" -> "Benutzerdefinierte Kategorie hinzufügen".
2. Füllen Sie "Kategoriename" aus, und erweitern Sie "Erweitert".
3. Verwenden Sie "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" im Fenster Regulärer Ausdruck.

Legen Sie diese Kategorie in den Zugriffsrichtlinien auf "Ablehnen" fest:

1. Navigieren Sie zu "Web Security Manager" -> "Access Policies" (Zugriffsrichtlinien).
2. Klicken Sie in der Spalte "URL-Kategorien" für die entsprechende Richtliniengruppe auf den Link.
3. Wählen Sie im Abschnitt "Benutzerdefinierte URL-Kategoriefilterung" für die neue Skype-Kategorie "Blockieren" aus.
4. Änderungen senden und bestätigen

Hinweis: Explizite CONNECT-Anfragen können nur blockiert werden, wenn der HTTPS-Proxydienst deaktiviert ist!

Wenn die WSA HTTPS-Entschlüsselung aktiviert ist, kann Skype-Datenverkehr höchstwahrscheinlich unterbrochen werden, da es sich nicht um reinen HTTPS-Datenverkehr handelt (trotz Verwendung von CONNECT und Port 443). Dies führt zu einem 502-Fehler, der von der WSA generiert wurde, und die Verbindung wird getrennt. Jeder echte HTTPS-Webdatenverkehr an eine IP-Adresse funktioniert weiterhin (wird jedoch auf der WSA entschlüsselt).

Blockieren von Skype - Explizite/transparente Umgebung mit aktiviertem HTTPS-Proxy

Erstellen Sie eine benutzerdefinierte Kategorie, die dem IP- und Port-443-Datenverkehr entspricht:

1. Navigieren Sie zu "Sicherheitsmanager" -> "Benutzerdefinierte URL-Kategorien" -> "Benutzerdefinierte Kategorie hinzufügen".
2. Füllen Sie "Kategoriename" aus, und erweitern Sie "Erweitert".
3. Verwenden Sie "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" im Fenster Regulärer Ausdruck.

Legen Sie diese Kategorie in den Entschlüsselungsrichtlinien fest, um sie zu entschlüsseln:

1. Navigieren Sie zu "Web Security Manager" -> "Entschlüsselungsrichtlinien".
2. Klicken Sie in der Spalte "URL-Kategorien" für die entsprechende Richtliniengruppe auf den Link.
3. Wählen Sie im Abschnitt "Benutzerdefinierte URL-Kategoriefilterung" für die neue Skype-Kategorie "Entschlüsseln" aus.
4. Senden und bestätigen Sie die Änderungen.

Hinweis: Da Skype-Datenverkehr an eine IP gesendet wird, wird er als Teil der "nicht kategorisierten URLs" betrachtet. Der gleiche Effekt wie oben tritt auf, je nachdem, ob die Aktion zur Entschlüsselung oder zum Durchlauf führt.