SIP Geräte hinter NAT

Einleitung

Wenn ein IP-Telefon hinter NAT (zb. einem Router) installiert wird, können Probleme durch das NAT-Gerät selbst, durch das Unvermögen des Telefons, seine eigene Netzwerkumgebung richtig zu verstehen, oder durch eine Kombination der beiden verursacht werden. Da es sich um ein so häufiges Problem handelt, verfügen die meisten IP-Telefone über integrierte Funktionen, die ihnen helfen, ihre eigene Netzwerkumgebung zu analysieren und Probleme beim NAT-Traversal zu lösen. Das wahrscheinlich nützlichste und effektivste ist der sogenannte STUN-Mechanismus. STUN wird im Folgenden näher erläutert. Eine weitere Möglichkeit, die einige IP-Telefone verwenden können, ist ICE. ICE funktioniert normalerweise in Verbindung mit STUN, wodurch das Telefon mehrere mögliche Kontaktadressen zu einem entfernten SIP-Server/SIP Telefonanlage anbieten kann. Wenn das Remote-SIP-Gerät eine Verbindung zu Ihrem Telefon herstellen möchte, kann es jede Kontaktadresse einzeln nacheinander versuchen, bis eine gefunden wird, die funktioniert.

STUN und ICE alleine reichen vielleicht nicht aus. Wie oben erwähnt, ist das Problem nicht nur, dass Ihr IP-Telefon es wissen muss, dass es hint er NAT ist. Es braucht manchmal auch Hilfe um durch das NAT-Gerät zu kommen oder sogar eine Verbindung herzustellen, die bereits über das NAT-Gerät hergestellt wurde. Insbesondere blockiert das NAT-Gerät möglicherweise alle eingehenden IP-Verbindungen zu Ihrem Telefon und verhindert dadurch, dass ein bidirektionaler Audiopfad hergestellt werden kann. Um dies zu umgehen, müssen Sie möglicherweise Port-Forwardings auf dem NAT / Firewall-Gerät verwenden. Ein Port-Forwarding ist ein wenig schwierig zu implementieren, besonders wenn Sie mehrere IP-Telefone hinter dem gleichen NAT / Firewall-Gerät haben. Das Lösen Ihrer NAT-Traversal-Probleme kann daher Konfigurationsänderungen am NAT-Gerät und am IP-Telefon erfordern.

STUN - Einfaches Durchlaufen von UDP über NAT

STUN - Simple Traversal von UDP über NAT

STUN ist ein Industriestandard (RFC389) für das Übersetzen von NAT. Es erfordert, dass Ihr IP-Telefon Zugang zu einem STUN-Server irgendwo im Internet hat. Zum Beispiel: "stun.l.google.com:19302". In dem folgenden Abschnitt wird erklärt, wie Sie auf Ihrem Telefon STUN verwenden können.

Eine einfache Erklärung, wie STUN funktioniert

Bevor Sie STUN verwenden können, muss Ihrem IP-Telefon die Adresse (oder URL) eines STUN-Servers irgendwo im Internet mitgeteilt werden. Wenn nun das Telefon eingeschaltet wird und noch bevor ein Registrierungsversuch unternommen wird, sendet das Telefon eine Reihe von Abfragen an den angegebenen STUN-Server. Der STUN-Server führt einige einfache Tests durch, um Dinge zu bestimmen: Ist das IP-Telefon hinter einem NAT-Gerät? Wie lautet die externe IP-Adresse des NAT-Geräts? Wie stark erzwingt das NAT-Gerät Regeln zum Blockieren eingehender UDP-Verbindungen? Macht es bei eingehenden Verbindungen einen Unterschied, ob eine ausgehende Verbindung zu dieser entfernten Adresse bereits hergestellt wurde? Es meldet dann die Ergebnisse an das IP-Telefon zurück. Das IP-Telefon ist nun in der Lage, diese Informationen zu verwenden, um die SIP-Nachrichten, die es bei der Registrierung sendet, zu ändern. Wenn Sie Glück haben, funktioniert nun alles einwandfrei.

Wie kann ich STUN benutzen?

Angenommen, Ihr IP-Telefon ist STUN-fähig. Die meisten IP-Telefone haben einen konfigurierbaren Parameter für die URL (oder IP-Adresse) des STUN-Servers. Oft müssen Sie nur eine gültige Adresse in dieses Feld eingeben, vielleicht ein Kontrollkästchen ankreuzen, das Telefon neu starten und das war es.

Die Adresse des STUN-Servers des Dienstanbieters kann manchmal durch eine spezielle DNS-Suche gefunden werden. Normalerweise haben IP-Telefone eine konfigurierbare Adresse für den STUN-Server. Wenn Sie jedoch keine in den Konfigurationsmenüs Ihres Telefons finden, kann STUN möglicherweise trotzdem verwendet werden, indem die Adresse automatisch von einem öffentlichen DNS-Server abgerufen wird. Sie müssen die Handbücher und Spezifikationen des Telefons konsultieren, um zu überprüfen, ob STUN auf diese Weise unterstützt wird.

Port-Weiterleitung

Port-Weiterleitung

Bei der Port-Weiterleitung konfigurieren Sie Ihr NAT / Firewall-Gerät so, dass bestimmte eingehende Verbindungen gezielt zu bestimmten Gerät im LAN (oder in der DMZ) zugelassen werden. Sie würden dies normalerweise tun, indem Sie eine Regel hinzufügen, die die Portnummer oder den Servicetyp für die externe WAN-Schnittstelle und die IP-Adresse des Zielservers im LAN angibt. In einigen Fällen kann die Regel auch die Portnummer angeben, die verwendet werden soll, wenn die Verbindung an den Host im LAN weitergeleitet wird - dies ermöglicht Port Address Translation oder PAT. Die meisten NAT / Firewall-Geräte erlauben Port-Forwarding. Die Funktion wird jedoch nicht unbedingt als "Portweiterleitung" bezeichnet. Manchmal ist es nur eine Firewall-Regel. manchmal benötigt es eine Firewall-Regel und eine NAT-Regel. Bei einigen Firewalls kann der eingehende Port der externen Schnittstelle einem anderen Port auf dem Zielhostgerät im LAN zugeordnet werden - der so genannten PAT. Andere erlauben nur die Verwendung derselben Portnummer für beide - bei Draytek-Routern heißt diese Option "Open Ports". Sie müssen daher mit den Konfigurationsoptionen Ihrer Firewall einigermaßen vertraut sein, bevor Sie versuchen, die Portweiterleitung einzurichten.

Wenn Sie mit SIP-Geräten hinter NAT arbeiten, müssen Sie möglicherweise folgende Ports für die Weiterleitung einrichten:
1. Der Haupt-SIP-Verbindungsport - normalerweise Port 5060/5061. Das Protokoll ist UDP und TCP.
2. Der RTP-Medienport oder die RTP-Port-Ports eine Reihe von höheren Portnummern (10.000 bis 20.000). Das Protokoll ist UDP.

Sie müssen herausfinden, welche Ports Ihr IP-Telefon für RTP-Medien verwendet. Die tatsächliche (n) Portnummer (n) sind normalerweise konfigurierbar. Sie sollten den Bereich der Portnummern auf so wenige wie nötig einstellen. Für ein IP-Telefon mit einer Leitung/Kanal benötigen Sie nur vier Anschlüsse. Sie sollten die Port-Weiterleitung für alle RTP-Ports plus eine weitere zusätzlich aktivieren, da RTP-Verbindungen normalerweise den Port numerisch oben für die Informationsrückmeldung (RTCP) verwenden. Man sollte für jedes Gerät 4 RTP Ports erlauben - separate Verbindungen können für Senden und Empfangen verwendet werden; Außerdem kann jede Verbindung einen Port für RTP und einen anderen für RTCP verwenden.

Versuchen Sie nach Möglichkeit, keine Portadressumsetzung zu verwenden. Wenn Sie jedoch mehr als ein IP-Telefon hinter demselben NAT-Gerät haben, können Sie feststellen, dass eine Portadressumsetzung fast unvermeidbar ist. Eine Alternative wäre, wenn mehrere statische IP-Adressen auf dem externen WAN-Port des NAT-Geräts konfiguriert sind. In diesem Fall können Sie für jedes Telefon 1: 1-NAT verwenden. Eine andere Möglichkeit besteht darin, den Standard-SIP-Port 5060 an jedem Telefon auf eine andere Nummer zurückzusetzen - dh, zwei IP-Telefone sollten nicht denselben SIP-Port verwenden. Außerdem müssen Sie sicherstellen, dass keine zwei IP-Telefone die gleichen RTP-Ports verwenden. Sie können dann Ihr Firewall- / NAT-Gerät so konfigurieren, dass eine Portweiterleitung für jedes Telefon ausgeführt wird, während die gleichen Portnummern am externen WAN-Port der Firewall beibehalten werden wie an jedem Telefon.

One-to-One-NAT

One-to-One-NAT kann eine sehr nützliche Lösung für VoIP-NAT-Traversal sein. Der Grund dafür ist, dass keine Portadressumsetzung erforderlich ist. Wenn Ihr IP-Telefon im SIP INVITE angibt, dass es auf Port 10005 nach RTP abhört, ist es einfach, das NAT-Gerät einzurichten, um Port 10005 an das IP-Telefon weiterzuleiten. In der Regel können die meisten Benutzeragenten (IP-Telefone) so konfiguriert werden, dass sie einen voreingestellten Bereich von Portnummern für die RTP-Mediensitzung verwenden. Gleiches gilt für SIP-Server hinter NAT - z. B. Asterisk - wo Sie den Bereich der Portnummern festlegen können, die für Mediensitzungen verwendet werden sollen. Nachdem Sie diesen Bereich von Portnummern definiert haben, müssen Sie das Firewall- / NAT-Gerät so einstellen, dass dieser Bereich von Ports an das IP-Telefon oder die Telefonanlage weitergeleitet wird.

Welche anderen Mechanismen erlauben es IP-Telefonen, hinter NAT zu verwenden?

Keep-Alive-Pakete

Viele SIP-Telefone verwenden "Keep-Alive" -Pakete, um die Verbindung aufrecht zu erhalten, die während der Registrierung des Telefons zuerst hergestellt wird. Bei der Registrierung handelt es sich um eine ausgehende Verbindung über das NAT-Gerät, so dass es im Allgemeinen problemlos funktioniert (da NAT-Firewalls generell ausgehende Verbindungen zulassen und nur eingehende blockieren). Sehen Sie in den Konfigurationsmenüs Ihres IP-Telefons nach, ob es eine "Keep Alive" -Option gibt. Falls ja, versuchen Sie es in einem Intervall von ca. 1 Minute einzustellen. Dies ist normalerweise ausreichend, um das NAT-Gerät dazu zu bringen, die Verbindung offen zu halten, und dies ermöglicht dem Server, SIP-Anfragen direkt an das registrierte Telefon zu senden. Es löst jedoch nicht das Problem, dass Verbindungen nicht über NAT eingehen können. Daher klingelt möglicherweise Ihr IP-Telefon, aber beim Beantworten des Anrufs ist kein Audio vorhanden oder es gibt eine 1-Wege-Audioverbindung.

Tipp: Verwechseln Sie das "keep-alive" -Intervall nicht mit dem "Re-registration" -Intervall. Letzteres ist die Zeit, die das Telefon wartet, bevor es eine weitere Registrierungsanforderung an den Server sendet. Sie sollten dies auf ein viel längeres Zeitintervall einstellen - zum Beispiel 30 oder sogar 60 Minuten -, um zu vermeiden, dass die Telefonanlage/SIP Server mit unnötigen Registrierungsversuchen überflutet wird.

Far-End-NAT-Traversal

Es ist für einen gut konzipierten SIP-Proxy- und Registrar-Server möglich, zu erkennen, dass ein entferntes IP-Telefon, das versucht, Verbindungen herzustellen oder Anrufe zu tätigen, tatsächlich hinter NAT steht und dies automatisch kompensiert. Dies wird "Far-End-NAT Traversal" genannt. Es beinhaltet Manipulation der SIP-Header, wenn sie auf dem Server ankommen und benötigt auch einen so genannten Media Proxy. Wenn Ihr Provider "Far-End-NAT Traversal" auf seinen Servern betreibt, ist es möglich, dass Sie STUN auf Ihrem Telefon deaktivieren müssen, damit der Host-Server ordnungsgemäß funktioniert.

Noch mehr Lösungen für NAT

Manuelle Einstellung der externen IP-Adresse

Einige VoIP-Geräte - Benutzeragenten und SIP-Server einschließlich Asterisk - haben konfigurierbare Parameter, die eine Option zur Angabe der IP-Adresse der externen Schnittstelle auf Ihrem NAT-Gerät enthalten. Wenn Ihre Asterisk PBX beispielsweise hinter NAT steht und Sie Probleme haben, SIP-Anrufe an externe Peers zu senden, können Sie wahrscheinlich das Problem lösen, indem Sie die externe IP-Adresse in Ihrer SIP.CONF-Datei angeben - den Parameter heißt "extern ip". Portweiterleitung kann ebenfalls erforderlich sein.

VPN

Einige Benutzer finden es bequem, eine VPN-Verbindung zu verwenden, um die Probleme der NAT-Traversierung zu überwinden. Dies ist sinnvoll für einen Heimarbeiter, der die VPN-Verbindung aus anderen Gründen benötigt und ein IP-Telefon verwenden möchte, das sich bei der PBX des Büros anmeldet. Die Verwendung von SIP über VPN kann jedoch auch Probleme verursachen, da der VPN-Mechanismus alle Pakete an einem Ende verschlüsselt und am anderen Ende entschlüsselt. Dieser Prozess ist sehr anspruchsvoll für die Ressourcen Ihres Computers oder vielleicht für die CPU-Ressourcen in der Firewall, die das VPN im Büro beendet. Wenn Ihr IP-Telefon Audio-Medien (Sprache) zwischen Heim und Büro überträgt, muss es viele Daten verschlüsseln und entschlüsseln. Dies kann Verzögerungen und CPU-Engpässe verursachen, die wiederum eine Verschlechterung der Sprachqualität verursachen, so dass einige Sorgfalt erforderlich ist. Na sicher,

SIP-fähige Firewalls

Einige Firewalls sind SIP-fähig. Dies bedeutet, dass sie so konfiguriert werden können, dass sie Pakete während der Übertragung prüfen und die in den SIP-Nachrichten eingebetteten IP-Adressen oder Portnummern durch die IP-Adresse und Portnummer ersetzen, die sie auf der externen WAN-Schnittstelle der Firewall öffnen. Eine gute Idee, wenn es funktioniert!

UPnP

Wenn die Firewall und das SIP-Gerät hinter der Firewall beide in der Lage sind, UPnP zu verwenden, kann es die richtige Lösung sein - sie können miteinander reden und sich hoffentlich darauf einigen, welche Ports geöffnet werden müssen, um SIP durchzulassen. Auch dies ist eine gute Idee, wenn es funktioniert, aber gehen Sie nicht davon aus, dass UPnP die Lösung für alle NAT-Traversal-Probleme ist.

Originaltext auf Englisch von: http://kb.smartvox.co.uk/voip-sip/sip-devices-nat