ویکی‌پدیا

STUN

این مقاله دقیق، کامل و صحیح ترجمه نشده و نیازمند ترجمه به فارسی است.

کل یا بخشی از این مقاله به زبانی به‌جز زبان فارسی نوشته شده‌است. اگر مقصود ارائهٔ مقاله برای مخاطبان زبان ترجم

بیشتر بدانید

STUN (**Session Traversal Utilities for NAT**) یک مجموعه استاندارد از روش ها شامل یک پروتکل شبکه ، برای عبور از دروازه های مترجم آدرس شبکه(NAT) در برنامه های صوتی ، ویدئویی ، پیام رسانی و سایر ارتباطات تعاملی است.

STUN ابزاری است که توسط پروتکل های دیگر مانند ایجاد ارتباط متقابل (ICE) ، پروتکل شروع جلسه (SIP) و WebRTC استفاده می شود. این ابزاری را برای میزبانان فراهم می کند تا حضور NAT ، آدرس پروتکل اینترنت (IP) و شماره درگاهی را که معمولاً عمومی است و همچنین نگاشت شده که NAT برای پروتکل کاربر داده ی برنامه (UDP) اختصاص داده است که به سمت میزبان حرکت می کند ، کشف کند. این پروتکل نیازمند کمک از سوی یک سرور شبکه شخص ثالث (سرور STUN) که واقع در طرف مخالف (عمومی) NAT قرار دارد که این معمولاً اینترنت عمومی می باشد.

در اصل ، STUN مخفف **Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators**[۱] می بود، اما این عنوان در توضیحات مجموعه به روز شده ای از روش ها که به صورت(RFC 5389 (https://datatracker.ietf.org/doc/html/rfc5389 انتشار یافت تغییر کرد ولی همان مخفف را حفظ کرده است. [۲]

طرح

STUN ابزاری برای پروتکل های ارتباطی به منظور شناسایی و پیمایش مترجمان آدرس شبکه است که در مسیر بین دو نقطه انتهایی ارتباط، قرار دارند.این به عنوان یک پروتکل سرویس گیرنده-سرور سبک پیاده سازی شده که فقط به اجزای پاسخ و پرس و جو ساده با یک سرور شخص ثالث واقع در شبکه مشترک و به راحتی قابل دسترس که به طور معمول

اینترنت است ،نیاز دارد. سمت مشتری در برنامه ارتباطات کاربر مانند تلفن (VoIP Voice over Internet Protocol) یا سرویس گیرنده پیام فوری پیاده سازی می شود.

پروتکل پایه به شرح زیر عمل می کند: گیرنده ، معمولاً در داخل یک شبکه خصوصی کار می کند که یک *درخواست الزام آور را* به یک سرور STUN در اینترنت عمومی ارسال می کند. سرور STUN ، همانطور که از دیدگاه سرور مشاهده می شود ، *با* یک *پاسخ موفقیت آمیز* که شامل آدرس IP و شماره پورت مشتری است، *پاسخ* می دهد.نتیجه از طریق نقشه برداری اختصاصی یا (XOR) با هدف دوری از ترجمه محتوای بسته توسط درگاه های لایه برنامه (ALG) که بازرسی بسته عمیق را انجام می دهند مبهم می شود.

پیام های STUN در بسته های (UDP User Datagram Protocol) ارسال می شوند. از آنجا که UDP حمل و نقل مطمئنی را فراهم نمی کند ، اطمینان این روش با انتقال مجدد درخواستهای STUN که توسط کنترل برنامه انجام می شود، بدست می آید. سرورهای STUN هیچ مکانیسم قابل اطمینانی برای پاسخ های خود، اجرا نمی کنند. [۲] وقتی اطمینان اجباری است ، ممکن است از پروتکل کنترل انتقال (TCP) استفاده شود ، اما باعث اضافه بار اضافی شبکه می شود. در برنامه هایی که نسبت به امنیت حساس می باشند ، STUN ممکن است توسط (TLS Transport Layer Security) حمل و رمزگذاری شود.

یک برنامه ممکن است به طور خودکار یک سرور STUN مناسب برای ارتباط با یک شخص خاص با پرس و جو از سیستم نام دامنه (DNS) برای *stun* (برای UDP) یا *stuns* (برای TCP / TLS) سرور (SRV) منبع ثبت ، به عنوان مثال _stun._udp.example.com. تعیین کند. شماره استاندارد درگاه گوش دادن برای یک سرور STUN برای UDP وTCP عدد 3478 و برای TLS، عدد 5349 می باشد. همچنین اگر پیاده سازی سرور بتواند بسته های TLS و STUN را چند برابر کند ، TLS ممکن است روی پورت TCP نیز اجرا شود. در صورت نیافتن سرور STUN، با استفاده از جستجوی DNS ، استاندارد توصیه می کند که نام دامنه مقصد باید برای سوابق آدرس (A یا AAAA) که با شماره درگاه پیش فرض استفاده می شود ، جستجو شود. [۲]

علاوه بر استفاده از رمزگذاری پروتکل با TLS، STUN همچنین از طریق انواع بسته های STUN تخصصی، دارای مکانیسم های احراز هویت داخلی و یکپارچگی پیام است.

هنگامی که یک گیرنده، آدرس خارجی خود را ارزیابی می کند ، می تواند از این طریق به اشتراک گذاری آدرس NAT خارجی به جای آدرس خصوصی که می تواند از طریق افراد دیگر در شبکه عمومی قابل دسترسی نباشد ، به عنوان کاندیدای ارتباط با همتایان خود استفاده کند.

اگر هر دو همتا ارتباط برقرار در شبکه های خصوصی مختلفی قرار دارند و هر کدام پشت NAT ، باید برای تعیین بهترین راه ارتباطی بین آنها هماهنگ شوند. برخی از رفتارهای NAT حتی ممکن است اتصال همگانی را محدود کنند حتی اگر اتصال عمومی مشخص باشد. پروتکل ایجاد ارتباط متقابل (ICE) مکانیسم ساختاری را برای تعیین مسیر ارتباطی بهینه بین دو Peer را فراهم می کند.برنامه های افزودنی پروتکل شروع جلسه(SIP) برای امکان استفاده از ICE هنگام تنظیم تماس بین دو میزبان تعریف شده اند.

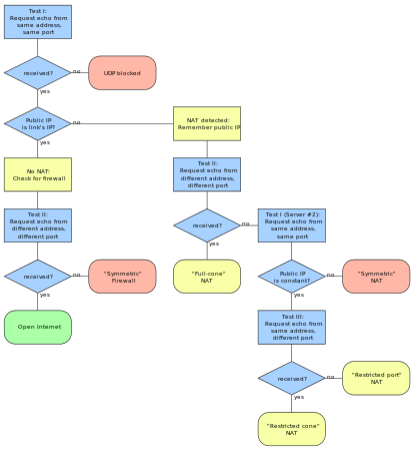
محدودیت ها

ترجمه آدرس شبکه از طریق چندین آدرس و طرح نگاشت پورت مختلف اجرا می شود که هیچ یک از آنها استاندارد نیست.

STUN یک راه حل پیمایشی جامع NAT نمی باشد که در همه سناریوهای استقرار NAT قابل استفاده باشد و با تمام آنها به درستی کار نمی کند. این یک ابزار در میان روش های دیگر است و ابزاری برای سایر پروتکل ها در مقابله با پیمایش NAT است که از جمله مهمترین آنها استفاده از پیمایش با استفاده از TURN (Relay NAT) و ایجاد ارتباط متقابل (ICE) می باشند.

STUN با سه نوع NAT کار می کند: مخروط کامل NAT ، مخروط محدود NAT و مخروط محدود پورت NAT . در موارد NAT مخروط محدود یا مخروط محدود پورت ، مشتری باید بسته ای را به نقطه انتهایی ارسال کند قبل از اینکه NAT بسته ها را از نقطه انتهایی به مشتری منتقل کند. STUN با NAT متقارن (که به آن NAT دو جهته نیز می گویند) که اغلب در شبکه های شرکت های بزرگ یافت می شود ، کار نمی کند. از آنجا که آدرس IP یک سرور STUN متفاوت از نقطه پایانی است ، در حالت NAT متقارن ، نگاشت NAT برای سرور STUN متفاوت از یک نقطه انتهایی خواهد بود. TURN با NAT متقارن نتایج بهتری را ارائه می دهد.

الگوریتم اصلی توصیف NAT



الگوریتم اصلی توصیف NAT از RFC 3489

مشخصات اصلی STUN در RFC 3489 ، الگوریتمی را برای توصیف رفتار NAT با توجه به آدرس و رفتار نگاشت پورت مشخص کرده است. این الگوریتم همیشه موفقیت آمیز نیست و فقط در زیر مجموعه ای از دستگاه های NAT قابل استفاده می باشد.

الگوریتم شامل یک سری از تستها می باشد که توسط یک برنامه اجرا می شود. هنگامی که مسیر درون نمودار به یک جعبه قرمز ختم می شود ، ارتباط UDP امکان پذیر نیست و وقتی مسیر به یک جعبه زرد یا سبز ختم می شود ، امکان برقراری ارتباط وجود دارد.

روش های RFC 3489 برای کنار آمدن با انبوهی از پیاده سازی های مختلف NAT و سناریوهای کاربردی که در شبکه های تولید وجود دارد ، بسیار غیر قابل اعتماد است. پروتکل و روش STUN در RFC 5389 بروز شد و بسیاری از مشخصات اصلی را به عنوان زیر مجموعه ای از روش ها حفظ کرد ، اما سایر موارد را حذف کرد.

همچنین ببینید

- پروتکل کنترل بندر
- سوراخ سوراخ UDP
- پروتکل دستگاه Gateway اینترنت

منابع

1. *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (http://tools.ietf.org/html/rfc3489) RFC 3489*
2. *Session Traversal Utilities for NAT (STUN) (http://tools.ietf.org/html/rfc5389) RFC 5389*

لینک های خارجی

- STUNTMAN - نرم افزار سرور منبع باز (http://www.stunprotocol.org/STUN)
- Yahoo VoIP STUN (https://www.youtube.com/watch?v=9MWYw0fltr0) در یوتیوب
- STUNT: TCP NAT traversal (https://web.archive.org/web/20170911122644/http://nutss.gforge.cis.cornell.edu/stunt.php) توسط Wayback Machine (بایگانی‌شده ۲۰۱۷-۰۹-۱۱)

آخرین ویرایش ۲ ماه پیش **توسط** ممد قولی **انجام شده**