بررسی اجمالی طراحی IPsec VPN WAN

این راهنمای طراحی، اجزای کاربردی جامع و مورد نیاز برای ساخت یک شبکه اختصاصی مجازی سایت به سایت (VPN) را در زمینه اتصال شبکه گسترده منطقه‌ای (WAN) تعریف می‌کند. این بررسی اجمالی درباره طراحی، در سطح بالا، انتخاب‌های طراحی دردسترس برای ساخت یک IPsec VPN WAN را تعریف می‌کند و عواملی را که بر انتخاب شما تأثیر می‌گذارند توصیف می‌کند. راهنمای طراحی فردی، طراحی و اجرای دقیق‌تر برای هر یک از انواع طراحی‌های اصلی را فراهم می‌کند.

بررسی اجمالی از طراحی، بخشی از راه‌حل‌های VPN در حال انجام را با استفاده از آخرین فناوری VPN از سیسکو و براساس اصول طراحی عملی که برای مقیاس‌گذاری مورد آزمایش قرار گرفته‌اند شناسایی می‌کند.

فهرست

بسته شدن پروتکل امنیتی

سرصفحه تایید (AH)

استفاده همزمان از ESP و AH

حالت‌های IPsec

حالت تونل

حالت حمل و نقل

کلید مبادله اینترنت

انجمن امنیتی

فاز اول IKE

فاز دوم IKE

مسائل مربوط به بخش‌بندی

تنظیم MTU روی کارت‌های رابط مشتری و سرور

مسیر پوشش داده شده توسط MTU

رابط MTU

قطعه‌بندی Look Ahead

حداکثر اندازه بخش TCP

چرا مشتریان IPsec VPN ها را راه‌اندازی می‌کنند

افراد حاضر در کسب و کار

پهنای باند

کاهش هزینه

امنیت

انعطاف‌پذیری

حالت ارتجاعی

نیازمندی‌های مشتری

رمزگذاری

تأیید هویت IKE

کیفیت خدمات

سطح رابط

سطح اتصال یا جلسه

چندپخشی IP

پروتکل‌های غیر IP

مسیریابی

دستیابی به‌صورت پویا

دسترسی زیاد

شکست Headend

عدم موفقیت سایت

شکست دفتر شعبه

شکست Stateful در مقابل stateless

امنیت مجتمع

مشبک کردن پویا

مقیاس‌پذیری

تامین و مدیریت

درک تکنولوژی

دسترسی بدون تماس

مدیریت در حال اجرا

ارائه‌دهنده خدمات

انتخاب طراحی

طراحی مستقیم بخش‌بندی IPsec

بررسی اجمالی

مزایا

معایب

بیشترین استفاده معمول

Point-to-Pint GRE برروی طراحی IPsec

معماری Headend در سطح دوجداره در مقابل سطح تک جداره

بررسی اجمالی طراحی

مزایا

معایب

بیشترین استفاده معمول

نقطه به نقطه GRE از طریق طراحی IPsec

معماری Headend-Headend تک لایه در مقابل Headend دوگانه

بررسی اجمالی طراحی

مزایا

معایب

بیشترین استفاده معمول

VPN پویای چند نقطه- توپولوژی طراحی Speoke-to-Speak VPN

بررسی اجمالی طراحی

مزایا

معایب

بیشترین استفاده معمول

طراحی رابط تونل مجازی

بررسی اجمالی طراحی

مزایا

معایب

بیشترین استفاده معمول

مقایسه طراحی

پشتیبانی از ویژگی‌های اصلی

پشتیبانی از پلت‌فرم

انتخاب طراحی

مقیاس‌پذیری یک طراحی

معیارهای بحرانی مقیاس‌پذیری

تعداد دفاتر شعبه

سرعت اتصال

نفوذ IPsec

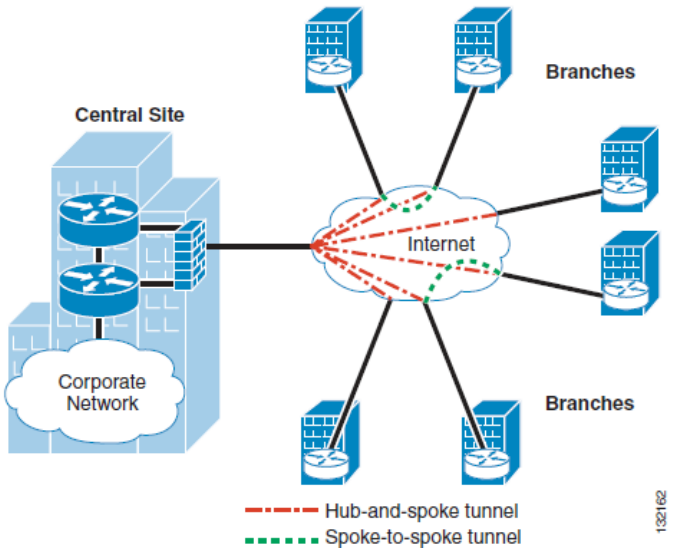
جفت‌های مسیریابی

معرفی

این متن به‌عنوان یک راهنمای طراحی برای کسانی است که قصد دارند یک VPN سایت به سایت براساس امنیت IP (IPsec) ارائه دهند. طرح‌های ارائه شده در این متن بر پلتفرم‌های روتر سیسکو IOS VPN تمرکز دارد.

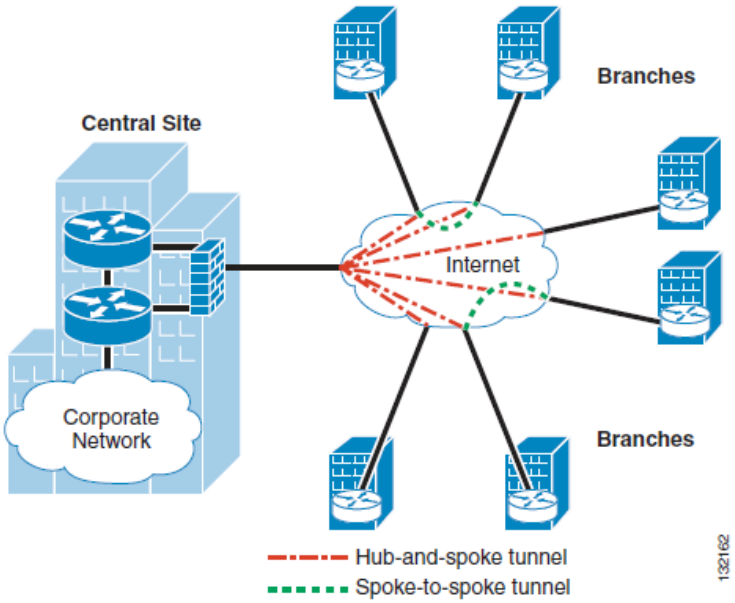
توپولوژی اولیه که در این متن توضیح داده شده است، یک طراحی hub-and-spoke است که منابع اولیه در یک سایت مرکزی بزرگ، با تعدادی سایت کوچک و یا دفاتر شعبه با اتصال مستقیم به سایت مرکزی بر روی یک VPN واقع شده‌اند. یک نمودار سطح بالا از این توپولوژی در شکل 1 نشان داده شده است.

شکل 1 توپولوژی hub-and-spoke VPN



معرفی توپولوژی VPN چندنقطه‌ای پویا (DMVPN)، یک طراحی با اتصال hub-and-spoke امکان‌پذیر با توانایی ایجاد ارتباط موقت بین سایت‌های گفتگو با استفاده از رمزگذاری IPsec فراهم می‌کند. این توپولوژی در شکل 2 نشان داده شده است.

شکل 2. توپولوژیSpoke-to-Spoke DMVPN VPN



این راهنمای طراحی با یک مرور کلی از راه‌حل‌های مختلف VPN آغاز می‌شود و به دنبال انتخاب معیارهای بحرانی و همچنین یک راهنما برای مقیاس‌پذیری یک راه‌حل است. در نهایت، یک مرور کلی از پلتفرم ارائه شده است.

مخاطب هدف

این راهنمای طراحی برای مهندسان سیستم طراحی شده است تا راهنمایی‌ها و بهترین شیوه‌ها را برای استقرار مشتری ارائه دهند.

محدوده کار

توپولوژی‌های طراحی زیر در حال حاضر جزء اهداف این راهنمای طراحی هستند:

- Encapsulation مستقیم IPsec
- Encapsulation مسیریابی عمومی (GRE) Point-to-Point (p2p) برروی IPsec
- VPN چندنقطه‌ای پویا (DMVPN)
- رابط مجازی تونل (VTI)

ویژگی‌های مهم و خدمات زیر در حال حاضر جزء اهداف این راهنمای طراحی هستند:

- تشخیص جفت‌های مرده (DPD)
- تزریق مسیر معکوس (RRI)
- تأیید هویت کلیدی اینترنت (IKE) با استفاده از امضای دیجیتال یا گواهی
- روتر سیسکو VPN در حال اجرا سیسکو IOS
- EIGRP و OSPF به‌عنوان پروتکل مسیریابی پروتکل داخلی (IGP) در سراسر VPN
- کیفیت خدمات (QoS) و صدا و ویدیو فعال شده با IPsec VPN (V3PN)
- پروتکل مسیریابی آماده به کار (HSRP) و سوئیچ (SSO) برای دسترسی بالا

• خدمات چندرسانه‌ای IP بر روی VPN

ویژگی‌های و خدمات زیر در حال حاضر خارج از محدوده اهداف این راهنمای طراحی هستند که این متن فراهم می‌کند:

• شناسایی آسان VPN و توپولوژی طراحی

• سیستم‌عامل‌های سیسکو غیر IOS شامل سری PIX و سری VPN3000

• برنامه‌های دسترسی از راه دور (مبتنی بر سرویس‌گیرنده)

• پروتکل‌های تونل‌زنی لایه 2 مانند پروتکل تونل لایه 2 (L2TPv3)، پروتکل تونل‌زنی نقطه به نقطه (PPTP) و WebVPN (SSL / TLS VPN ها)

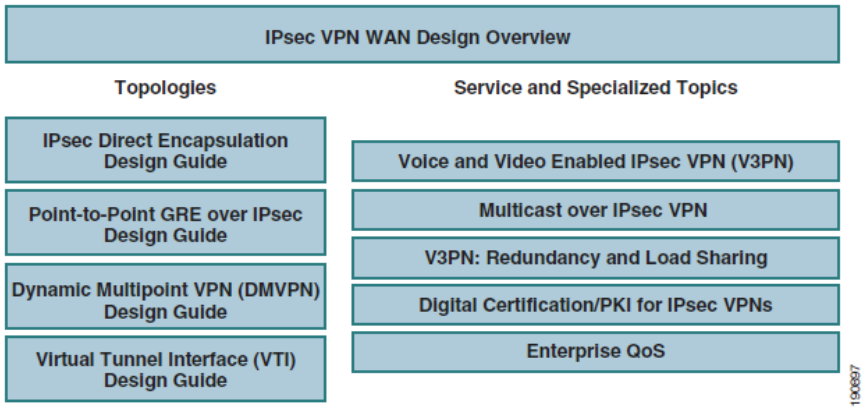
• VPN های مبتنی بر MPLS

• مدیریت شبکه

ساختار طراحی راهنمای

این راهنما بخشی از مجموعه راهنماهای طراحی است که هر کدام براساس فن‌آوری‌های مختلف برای معماری IPsec VPN WAN هستند (به شکل 3 نگاه کنید). هر تکنولوژی از IPsec به‌عنوان مکانیزم حمل و نقل برای هر VPN استفاده می‌کند.

شکل 3 راهنمای طراحی IPsec VPN WAN



استفاده از IPsec در این راهنما به خوبی انتخاب معیارهای خاص IPsec VPN در تکنولوژی WAN مشخص شده است.

بررسی اجمالی IP امنیتی

هدف از این بررسی، معرفی امنیتIP (IPsec) و کاربرد آن در VPN ها است. برای درک عمیق IPsec، به آدرس زیر مراجعه کنید:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml

معرفی IPsec

استاندارد IPsec یک روش برای مدیریت احراز هویت و حفاظت از داده‌ها بین جفت‌های رمزنگاری شده در انتقال امن اطلاعات را فراهم می‌کند. IPsec شامل انجمن امنیت اینترنت و پروتکل مدیریت کلید Oakley / (ISAKMP) و دو پروتکل IPsec IP است:encapsulating پروتکل امنیتی (ESP) و سرآیند تایید (AH).

IPsec از الگوریتم‌های رمزنگاری متقارن برای حفاظت از داده‌ها استفاده می‌کند. الگوریتم‌های رمزنگاری متقارن برای پیاده‌سازی روی سخت‌افزار کارآ و راحت هستند. این الگوریتم‌ها نیاز به روش امن کلید تبادل برای اطمینان از حفاظت داده‌ها دارند. پروتکل‌های ISAKMP / Oakley این قابلیت را فراهم می‌کنند.

این راه‌حل مستلزم یک روش مبتنی بر استاندارد برای محافظت از داده‌ها در مقابل استراق سمع و اصلاح است. IPsec چنین روشی را فراهم می‌کند. IPsec انتخاب مجموعه‌های تبدیل را فراهم می‌کند تا کاربر بتواند قدرت حفاظت از اطلاعات را داشته باشد. IPsec همچنین دارای چندین کد تایید هویت (HMAC) انتخابی است، که هر کدام دارای سطوح مختلف حفاظت از حملات مانند man-in-the-middle، جواب بسته (ضد جواب) و حملات یکپارچه اطلاعات هستند.

پروتکل‌های تونل‌زنی

پروتکل‌های تونل‌زنی در ویژگی‌هایی که پشتیبانی می‌کنند، مشکلاتی که برای حل آنها طراحی شده‌اند و مقدار امنیتی که برای انتقال داده ارائه می‌کنند متفاوت هستند. طرح‌های ارائه شده در این معماری براستفاده از IPsec به‌عنوان پروتکل تونل‌زنی، IPsec مورد استفاده در ارتباط باEncapsulation مسیریابی عمومی(GRE) و رابط‌های مجازی تونل (VTI) تمرکز دارند.

هنگامی که به‌تنهایی استفاده می‌شود، IPsec یک شبکه خصوصی و انعطاف‌پذیر برای یکپارچه‌سازی IP فراهم می‌کند، جایی که پشتیبانی برای چندپخشی IP، پروتکل مسیریابی IGP پویا، یا پروتکل‌های غیر IP مورد نیاز نیست. هنگامی که از یکی یا تعداد زیادی از این ویژگی‌ها مورد نیاز باشد، IPsec باید همراه با GRE یا VTI استفاده شود.

طراحی P2P GRE بر روی IPsec هر سه ویژگی که در پاراگراف قبلی شرح داده شده است را امکان‌پذیر می‌کند، درحالی‌که طراحی DMVPN یا طراحی VTI تنها الزامات پروتکل مسیریابی IGP و IP multicast را اجرا می‌کنند.

سایر پروتکل‌های تونل‌زنی ممکن شامل موارد زیر هستند:

- لایه امنیت سوکت/ امنیت لایه انتقال (SSL / TLS)
- VPN (WebVPN)
- پروتکل تونل‌زنی نقطه به نقطه (PPTP)
- لایه دوم پروتکل تونل‌زنی (L2TP)

این پروتکل‌ها بر اساس اتصالات VPN کاربر یا سرویس‌گیرنده به دروازه هستند که معمولا با نام راه‌حل‌های دسترسی از راه دور شناخته می‌شوند و در این راه‌حل اجرا نمی‌شوند.

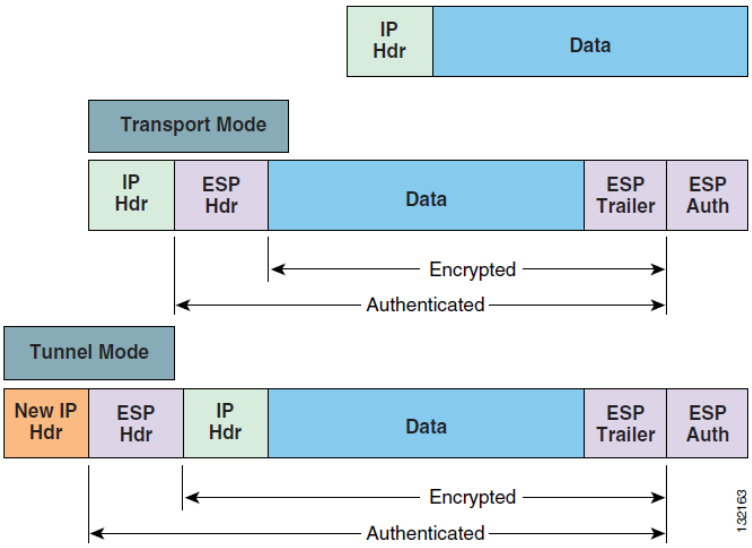
پروتکل‌های IPsec

بخش‌های زیر دو پروتکل IP مورد استفاده در استاندارد IPsec را شرح می‌دهند: ESP و AH.

بسته شدن پروتکل امنیتی

هدر ESP (IP پروتکل 50) هسته پروتکل IPsec را تشکیل می‌دهد. این پروتکل، در رابطه با یک مجموعه توافق شده از پارامترهای امنیتی یا مجموعه انتقال، داده‌ها را با شناسایی آنها محافظت می‌کند. این پروتکل تنها بخش داده‌های بسته را رمزگذاری می‌کند و از دیگر محافظت‌ها (HMAC) برای دیگر حفاظت‌ها (یکپارچگی اطلاعات، ضد پاسخ، man-in-the-middle) استفاده می‌کند. به صورت اختیاری می‌توان آن را برای احراز هویت داده‌های محافظت شده نیز ارائه کرد. شکل 4 نشان می‌دهد که چگونه ESP یک بسته IP را محصور می‌کند.

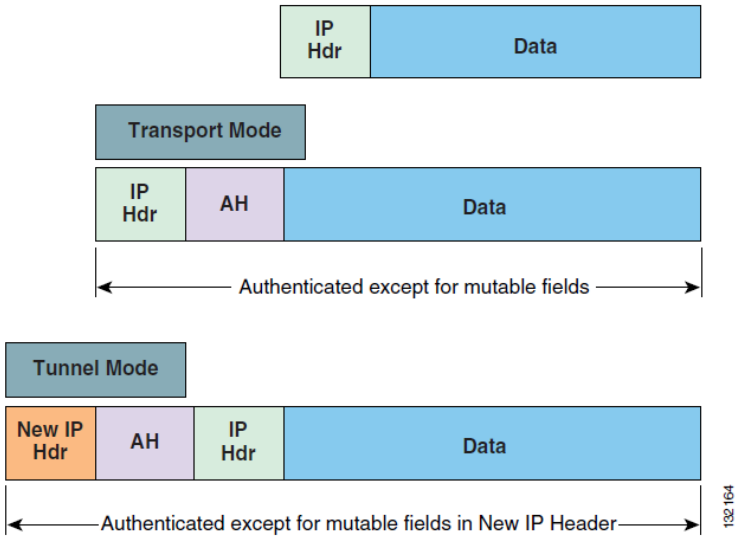
شکل 4 پروتکل امنیتیEncapsulating (ESP)



سرصفحه تایید (AH)

پروتکل AH (IPپروتکل 51) بخش دیگری از IPsec را تشکیل می‌دهد. AH اطلاعات را در فایل با پنهان کردن داده‌ها به‌صورت معمول رمزگذاری نمی‌کند، اما یک مهر و موم مشخص به داده‌ها اضافه می‌کند. همچنین از زمینه‌های غیر قابل تغییر در هدر IP حمل داده‌ها محافظت می‌کند، که شامل هدر IP است. پروتکل AH در صورتی که نیاز به محرمانه بودن اطلاعات باشد نباید به تنهایی مورد استفاده قرار گیرد. شکل 5 نشان می‌دهد که چگونه AH یک بسته IP را کپسوله می‌کند.

شکل 5. سرآیند تایید (AH)



استفاده همزمان از ESP و AH

امکان استفاده همزمان از ESP و AH در انجمن امنیتی IPsec (SA) یکسان وجود دارد. ESP شامل احراز هویت یکسانی به عنوان AH است وهمچنین رمزگذاری و حفاظت از داده‌ها را فراهم می‌کند. فقط استفاده از ESP در معماری توصیف شده در این راهنما نشان داده شده است.

حالت‌های IPsec

IPsec دو حالت زیر را برای ارسال داده در یک شبکه دارد:

- حالت تونل
- حالت حمل و نقل

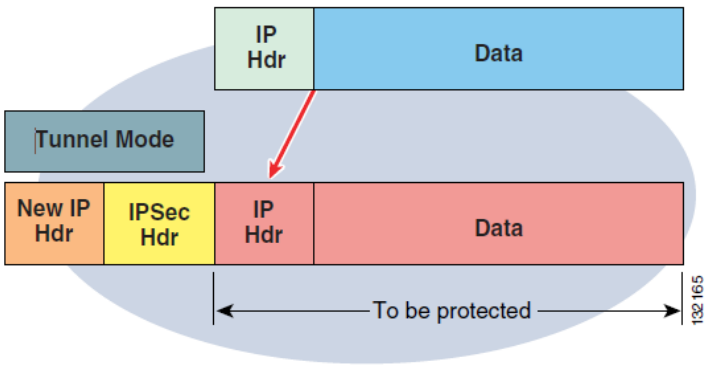
عملکرد هر کدام بنا به مقدار سربار اضافه شده به بسته متفاوت است. این حالت‌ها در دو بخش بعدی با جزئیات شرح داده می‌شود.

حالت تونل

حالت تونل با بسته‌بندی و حفاظت از کل بسته IP عمل می‌کند. از آنجا که حالت تونل هدر IP بسته را قبل از رمزگذاری پنهان می‌کند، هدر جدید IP اضافه می‌شود به طوری که بسته با موفقیت ارسال شود. دستگاه‌های رمزنگاری خودشان IP مورد استفاده در هدر جدید را مشخص می‌کنند. این آدرس‌ها را می‌توان در پیکربندی روترهای IOS سیسکو مشخص کرد. حالت تونل می‌تواند با هر یک یا هر دو پروتکل IPsec (ESP و AH) استفاده شود. حالت تونل در نتیجه گسترش بسته به دلیل هدر IP جدید حدود 20 بایت است. حالت تونل به طور گسترده‌ای امن‌تر و انعطاف‌پذیرتر از حالت حمل و نقل است. حالت تونل IPsec منبع و آدرس‌های IP مقصد در بسته اصلی را رمزگذاری می‌کند و اطلاعات را از شبکه محافظت نشده پنهان می‌کند. این مورد به جلوگیری از حملات مهندسی اجتماعی کمک می‌کند.

شکل 6 گسترش بسته‌های IP را نشان می‌دهد.

شکل 6 حالت تونل IPsec



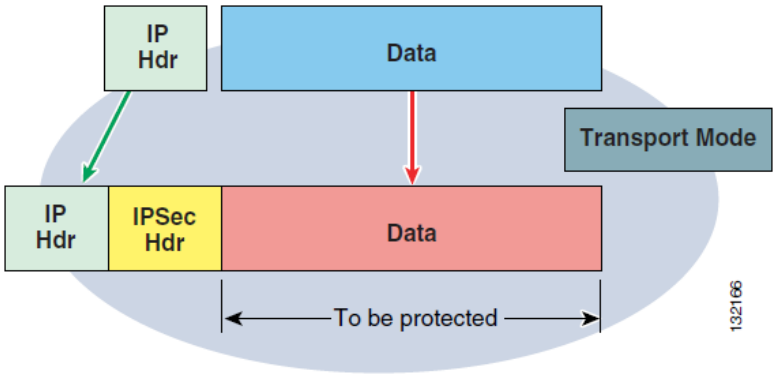
حالت حمل و نقل

حالت حمل و نقل IPsec با قرار دادن سرصفحه ESP یا AH بین هدر IP و پروتکل بعدی یا لایه انتقال بسته کار می‌کند. هر دو IP دو گره از شبکه را نشان می‌دهند که ترافیک آنها توسط IPsec در هدر IP بسته که پس از رمزگذاری قابل مشاهده است محافظت می‌شود. این حالت IPsec می‌تواند حساس به حملات تجزیه و تحلیل ترافیک باشد. بااین حال، چرا هیچ هدر IP اضافی اضافه نشده است، زیرا نتیجه این مورد انبساط بسته را کاهش می‌دهد. حالت حمل و

نقل را می‌توان با یک یا هر دو ESP و AH اعمال کرد. حالت حمل و نقل را می‌توان با P2P GRE بر روی IPsec استفاده کرد، زیرا این طراحی آدرس انتهایی را با اضافه کردن سرصفحه IP خود پنهان می‌کند. اگر آدرس IP منبع یا آدرس IP مقصد آدرس سازگار RFC 1918 باشد، بسته نمی‌تواند در اینترنت عمومی منتقل شود، و این آدرس‌ها نمی‌توانند یک آدرس شبکه (NAT) یا پورت آدرس ترجمه (PAT) را بدون عدم اعتبار HMAC بسته رمزنگاری انتقال دهند.

شکل 7 گسترش بسته‌های IP را نشان می‌دهد.

شکل 7 حالت حمل و نقل IPsec



تبادل کلید اینترنت

برای پیاده‌سازی یک راه حل VPN با رمزگذاری، تغییر دوره‌ای کلید رمزگذاری جلسه ضروری است. عدم تغییر این کلید باعث می‌شود که VPN به حملات رمزگشایی شدید دست یابد. IPsec مشکل را با پروتکل IKE حل می‌کند که از دو پروتکل دیگر برای احراز هویت یک peer و برای تولید کلیدها استفاده می‌کند. IKE از یک الگوریتم ریاضی به نام مبادله دیفی-هلمن برای تولید کلیدهای جلسه متقارن استفاده می‌کند که توسط دو نفر از همتایان رمزنگاری استفاده شده است. همچنین IKE مذاکره را مانند پارامترهای امنیتی نظیر اطلاعات محافظت شده، قدرت کلیدها، روش‌های هش استفاده شده و این که آیا بسته‌ها از ضد پاسخ محافظت می‌شوند، مدیریت می‌کند. ISAKMP معمولا از پورت 500 پورت UDP به عنوان هر دو پورت منبع و مقصد استفاده می‌کند.

انجمن امنیتی

یک انجمن امنیتی (SA) یک توافق دو طرفه درگیر در مبادله رمزنگاری است. این توافق شامل نوع و قدرت الگوریتم رمزنگاری مورد استفاده برای حفاظت از داده‌ها است. SA شامل روش و قدرت احراز هویت داده‌ها و روش ایجاد کلیدهای جدید برای حفاظت از داده‌ها است. همتایان رمزنگاری در بخش زیر شرح داده شده اند.

هر SA دارای یک مقدار طول عمر است تا یک SA معتبر در نظر گرفته شده است. مقدار طول عمر با هر دو معیار زمان (ثانیه) و حجم (تعداد بایت) اندازه‌گیری می‌شود و در ایجاد SA مورد مذاکره است. این دو طول عمر مقایسه می‌شوند و توافق بر روی پایین‌ترین مقدار صورت می‌گیرد. تحت شرایط عادی، مقدار طول عمر از طریق زمان قبل از محدودیت حجم، منقضی می‌شود. بنابراین، اگر یک بسته جالب در 120 ثانیه آخر عمر مقدار یک SA فعال با SA منطبق باشد، فرآیند بازیابی رمزگشایی به طور معمول فراخوانده می‌شود تا فرآیند کلید رمزنگاری دیگری برای یک SA فعال قبل از حذف SA موجود ایجاد کند. این نتیجه، یک انتقال صاف با حداقل دستکاری بسته به SA جدید است.

انجمن امنیتی ISAKMP

ISAKMP SA یک کانال مذاکره امن دوطرفه است که توسط همتایان رمزنگاری برای ارتباطات پارامترهای مهم امنیتی با یکدیگر، مانند پارامترهای امنیتی IPsec(تونل داده) استفاده می‌شود.

در IOS سیسکو، سیاست ISAKMP SA طول عمر پیش فرض 86،400 ثانیه بدون محدودیت حجم دارد.

انجمن امنیت IPsec (تونل داده)

IPsec SA یک کانال ارتباطی یک طرفه بین یک peer با دیگری است. اطلاعات واقعی مشتری فقط یک IPsec SA است و هرگز بیش از ISAKMP SA نمی‌تواند باشد. هر طرف تونل IPsec یک جفت IPsec SA برای هر اتصال دارد یکی از راه دور، یکی برای راه دور. این جفت اطلاعات IPsec SA به صورت محلی در پایگاه داده SA ذخیره می‌شوند.

در IOS سیسکو، سیاست IPsec SA طول عمر پیش فرض 3600 ثانیه با 4،608،000 کیلوبایت محدودیت حجم دارد.

فاز اول IKE

فاز اول IKE، مذاکرات اولیه و دو طرفه ISAKMP SA بین دو جفت رمزنگاری شده به عنوان حالت اصلی اشاره شده است. فاز اولIKE با احراز هویتی که در آن هر جفت رمزنگاری هویت خود را با یکدیگر بررسی می‌کنند شروع می‌شود. هنگام تأیید اعتبار، جفت رمزنگاری شده در مورد الگوریتم رمزگذاری، روش هش و سایر پارامترهای توصیف شده در بخش‌های زیر برای ساخت ISAKMP SA موافق هستند. مکالمه بین دو جفت رمزنگاری می‌تواند با رفع نگرانی از بازیابی کلید به هنگام تماس استعلام شود. ISAKMP SA توسط فرایند IKE برای مذاکره با امنیت در پارامترهای IPsec SA استفاده می‌شود. اطلاعات ISAKMP SA به صورت محلی در پایگاه داده SA هر یک ذخیره می‌شود. جدول 1 پارامترهای مختلف امنیتی تعریف شده در بخش‌های زیر را نشان می‌دهد.

جدول 1. پارامترهای امنیتی ISAKMP SA

Default in Cisco IOS	Authentication	Encryption	HMAC	Diffie-Hellman	Lifetimes	NAT-T
ISAKMP SA parameters	RSA signatures (PKI) (default)	DES (default)	SHA-1 (default)	Group 1 (default)	86,400 seconds No volume limit (default)	Enabled (default)
	PSK	3DES	MDS	Group 2	User definable	Disabled
	RSA nonce	AES 128		Group 5		
		AES 192				
		AES 256				

روشهای تأیید اعتبار

فاز اول IKE دارای سه روش تأیید اعتبار است: کلیدهای پیش از اشتراک (PSK)، کلید عمومی زیرساخت (PKI) با استفاده از گواهی‌های دیجیتال X.509 و nonces رمزگذاری شده RSA. برای این هدف معماری، فقط PSK و PKI

با گواهینامه‌های دیجیتال X.509 شرح داده شده است، اما طراحی با هر یک از این روش‌های تأیید اعتبار امکان‌پذیر است.

کلیدهای پیش از اشتراک

PSK ها یک رشته کلید از پیش تعیین شده در هر جفت رمزنگاری هستند که برای شناسایی یکدیگر استفاده می‌شوند. به هنگام استفاده از PSK، دو جفت رمزنگاری قادر به مذاکره و ایجاد ISAKMP SA هستند. PSK معمولا حاوی آدرس آی پی میزبان یا زیر شبکه و ماسک است که برای PSK خاص معتبر است. یک کلمه PSK نوع خاصی از PSK است که شبکه و ماسک می‌تواند هر آدرس IP باشد.

زیرساخت کلید عمومی با استفاده از گواهینامه‌های دیجیتال X.509

جایگزینی برای اجرای PSK، استفاده از زیرساخت کلید عمومی (PKI) با گواهینامه‌های دیجیتال X.509است. گواهینامه‌های دیجیتال از یک شخص ثالث مورد اعتماد استفاده می‌کنند، که به عنوان یک گواهینامه معتبر شناخته می‌شوند (CA) و به صورت دیجیتالی، قسمت عمومی کلید nonce رمزگذاری شده را امضا می‌کنند.

همراه با گواهینامه، یک نام، شماره سریال، مدت اعتبار و سایر اطلاعاتی که IPsec دستگاه می‌تواند برای تعیین اعتبار گواهی استفاده کند وجود دارد. همچنین گواهی‌نامه می‌تواند لغو شود.

پیکربندی و مدیریت گواهینامه‌های دیجیتال با جزئیات در صدور گواهینامه دیجیتال / راهنمای طراحیPKI برای IPsec VPN در آدرس زیر پوشش داده شده است:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/DCertPKI.html

الگوریتم های رمزگذاری

رمزنگاری از الگوریتم‌های رمزنگاری مختلف استفاده می‌کند. در هسته الگوریتم رمزنگاری یک کلید مخفی مشترک برای تأیید اعتبار هر جفت وجود دارد. هنگام تایید هویت، داده‌های متنی با طول ثابت به الگوریتم وارد می‌شوند و به متن رمز تبدیل می‌شوند. متن رمزنگاری با استفاده از ESP به جفت رمزنگاری منتقل می‌شود. جفت بسته‌های ESP را دریافت می‌کند، متن رمز را استخراج می‌کند، آن را از طریق الگوریتم رمزگشایی اجرا می‌کند و یک متن واضح را برای همان ورودی بر روی peer رمزگذاری به خروجی می‌فرستد.

IOS سیسکو از DES، DES3، AES 128، AES 192 و الگوریتم‌های رمزنگاری AES 256 با DES طراحی شده به عنوان پیش فرض پشتیبانی می‌کند.

کدهای اعتبارسنجی پیام هشدار

الگوریتم‌های هش اساسی که توسط حالت اصلی استفاده می‌شوند، پیام رمزنگاری Digest 5 (MD5) و توابع هش الگوریتم امنیت هش 1 (SHA-1) هستند. الگوریتم‌های هش به صورت تکامل یافته در کدهای تأیید هویت پیام (HMAC) به کار گرفته شده‌اند، که امنیت ثابت شده هش کردن را با توابع رمزنگاری اضافی ترکیب می‌کنند. هش تولید شده با کلید خصوصی فرستنده رمزگذاری شده است.

MD5 و SHA-1 در داخل IOS Cisco، با SHA-1 به‌عنوان پیش فرض پشتیبانی می‌شوند.

توافقنامه کلید Diffie-Hellma

توافق کلید Diffie-Hellman یک روش رمزگذاری کلید عمومی است که راه‌حلی برای دو رمزنگاری برای ایجاد یک کلید مخفی مشترک که تنها آنها می‌دانند فراهم می‌کند، در حالی که در ارتباط با یک کانال ناامن است.

با کلید اختیاری Diffie-Hellman، هر جفت یک کلیدی عمومی و خصوصی تولید می‌کند. کلید خصوصی تولید شده توسط هر جفت مخفی نگه داشته می‌شود و هرگز به اشتراک گذاشته نمی‌شود. کلید عمومی از کلید خصوصی

توسط هر جفت محاسبه می‌شود و بر روی کانال ناامن مبادله می‌شود. هر جفت، کلیدهای عمومی را با کلید خصوصی شخصی خود ترکیب می‌کند و یک عدد مخفی مشترک را محاسبه می‌کند. سپس عدد مخفی مشترک به یک کلید مخفی مشترک تبدیل می‌شود. کلید مخفی مشترک هرگز بر روی کانال ناامن مبادله نمی‌شود.

گروه‌های Diffie-Hellman، 1، 2 و 5 در Cisco IOS پشتیبانی می‌شوند. گروه 1 مقدار پیش‌فرض با طول کلید 768 بیت است. گروه 2 طول کلید 1024 بیت دارد و گروه 5 دارای طول کلیدی 1536 بیتی است.

شفافیت NAT (تراکم NAT)

شفافیت IPsec NAT (NAT-T)، جفت رمزنگاری برای انتقال از طریق نقاط NAT یا PAT در شبکه با بسته‌بندی بسته‌های رمزنگاری در بسته‌بندی UDP معرفی می‌کند، که اجازه می‌دهد بسته‌ها از دستگاه‌های NAT عبور کنند. NAT-T برای اولین بار در سیسکو IOS 12.2 (13) T معرفی شد و به طور پیش فرض به‌عنوان یک دستور جهانی معرفی شد. NAT-T به صورت خودکار بین دو جفت رمزنگاری در هنگام مذاکره ISAKMP با یک پورت UDP مقصد از 4500 مذاکره می‌کند. منبع از پورت بالاتر در دسترس استفاده می‌کند. هنگامی‌که پورت UDP 4500 استفاده می‌شود، پورت مقصد به پورت 4501، 4502 و غیره حرکت می‌کند تا یک جلسه ISAKMP ایجاد شود. NAT-T در RFC 3947 تعریف شده است.

فاز دومIKE

در مرحله دوم IKE، IPsec SA با فرایند IKE و با استفاده از ISAKMP دو طرفه مذاکره می‌کند و اغلب به حالت سریع اشاره می‌شود. IPsec SA در طبیعت یک جانبه است و باعث ایجاد یک کلید جداگانه برای مبادله داده‌های جریان در هر جهت می‌شود. یکی از مزایای این استراتژی این است که میزان کار مورد نیاز برای موفقیت دو طرفه در یک مکالمه دو برابر است. در حین حالت سریع فرایند مذاکره، جفت رمزنگاری در مورد مجموعه‌های تبدیل، روش‌های هش، و پارامترهای دیگر موافق هستند. جدول 2 پارامترهای مختلف امنیتی را نشان می‌دهد.

جدول 2. پارامترهی امنیتی IPsec SA

Default in Cisco IOS	Encryption	HMAC	PFS	Lifetimes	IPsec Mode
IPsec SA parameters	DES (default)	SHA-1 (default)	Disabled (default)	3600 seconds 4,608,000 Kbytes (default)	Tunnel mode (default)
	3DES	MD5	Group 1	User definable	Transport mode
	AES 128		Group 2		
	AES 192		Group 5		
	AES 256				

الگوریتم‌های رمزگذاری

همانند حالت اصلی، حالت سریع از الگوریتم رمزنگاری برای ایجاد IPsec SA استفاده می‌کند. الگوریتم رمزگذاری مذکور توسط فرآیند حالت سریع می‌تواند یکسان یا متفاوت از آن در فرآیند حالت اصلی باشد. IOS سیسکو از الگوریتم‌های رمزگذاری DES، DES3، AES 128، AES 192 و AES 256، با DES به‌عنوان پیش فرض پشتیبانی می‌کند.

کدهای اعتباربخشی پیام هشدار

همانند حالت اصلی، حالت سریع از HMAC برای ایجاد IPsec SA استفاده می‌کند. HMAC مذکور توسط فرایند حالت سریع می‌تواند یکسان یا متفاوت از فرآیند حالت اصلی باشد. MD5 و SHA-1 در Cisco IOS، با SHA-1 به‌عنوان پیش فرض پشتیبانی می‌شوند.

پنهان نگه داشتن کامل

اگر پنهان نگه داشتن کامل (PFS) در سیاست IPsec مشخص شده باشد، تبادل جدید Diffie-Hellman با هر حالت سریع مذاکره قابل انجام است و مواردی با آنتروپی بزرگتر را فراهم می‌کند و در نتیجه مقاومت بیشتری نسبت

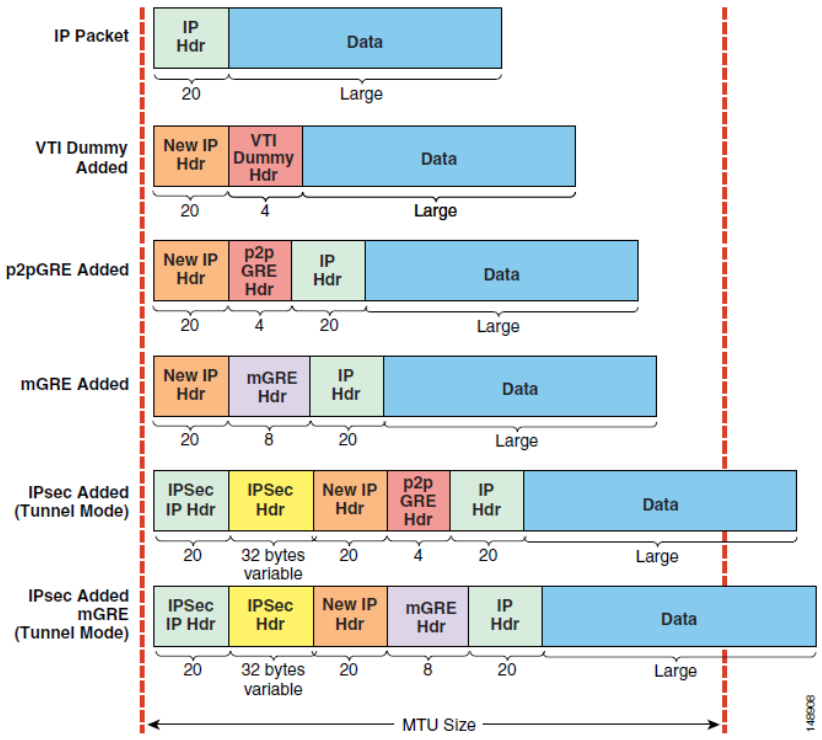
به حملات رمزنگاری دارد. هر مبادله دیفی هالمن نیاز به انعطاف‌پذیری بالایی دارد، در نتیجه موجب افزایش استفاده از CPU و پرداخت هزینه عملکرد می‌گردد.

گروه 1، 2، و 3 PFS (Diffie-Hellman) در Cisco IOS پشتیبانی می‌شوند. PFS به طور پیش فرض غیرفعال است. گروه 1 طول کلید 768 بیتی دارد، گروه 2 طول کلید 1024 بیتی و گروه 5 دارای طول کلید 1536 بیتی است.

مسائل قطعه بندی

طرح‌های مختلف IPsec VPN از محفظه دیتاگرام اصلی IP و با استفاده از موارد زیر استفاده می‌کنند: طراحی Encapsulationمستقیم IPsec، Point-to-Point GRE بر روی طراحی IPsec، طراحی DMVPN (mGRE) یا طراحی VTI. این بسته‌بندی‌ها به اندازه بسته اصلی اضافه می‌شوند. شکل 8 بسته‌های مختلف را نشان می‌دهد.

شکل 8 توسعه بسته‌های مختلف



هنگامی که یک بسته فراتر از حداکثر واحد انتقال (MTU) باشد، روتر آغازگر باید قبل از انتقال بسته تقسیم شود، یعنی روتر دریافت کننده باید دوباره قطعات را قبل از رمزگشایی جمع‌آوری کند. فرایند بازآموزی معمولا در سطح پردازش برنامه انجام می‌شود، که به‌طور جدی بر عملکرد روتر تاثیر می‌گذارد. بنابراین، از تقسیم‌بندی باید اجتناب شود اگر ممکن باشد. چندین گزینه برای جلوگیری از تکه تکه شدن وجود دارد، برخی از آنها در Cisco IOS پیکربندی شده‌اند و برخی از آنها نیاز به تغییر در مشتریان VPN و یا ایستگاه های پایان یافته دارند.

تنظیم MTU بر روی کارت‌های رابط مشتری و سرور

بهترین راه برای جلوگیری از مسائل قطعی در یک محیط VPN تنظیم دستی MTU بر روی کارت واسط شبکه مشتری و سرور (NIC) به مقدار کوچکتر از استاندارد با ارزش1500 بایت برای استفاده 1300 بایت است. بااین حال، به دلیل اینکه متوسط شبکه سازمانی به‌طور بالقوه هزاران ایستگاه کاری از کلاینت‌ها دارد، این کار همیشه امکان‌پذیر نیست. دومین استراتژی تنظیم MTU بر روی NIC در برنامه سرورها به 1300 بایت است، زیرا این دستگاه‌ها معمولا در یک مکان امن برای مدیران شبکه قابل دسترس هستند و به این دلیل اغلب بزرگترین بسته‌ها را اداره می‌کنند.

مسیر پوشش داده شده توسط MTU

یکی از ویژگی‌های IP با نام مسیر پوشش داده شده توسطMTU (PMTUD) است که می‌تواند احتمال تقسیم شدن را توسط ایستگاه‌های انتهایی که پشتیبانی می‌کنند از بین ببرد. این ویژگی می‌تواند کوچکترین MTU بین دو ایستگاه انتهایی را برای اطمینان از اینکه فرستنده یک بسته را که نتیجه تقسیم‌بندی است ارسال نمی‌کند، تعیین کند.
با فعال کردن PMTUD، تمام بسته‌ها با مجموعه‌ای از بیت‌های بدون قطعه‌بندی (DF) ارسال می‌شوند. اگر یک بسته با یک لینک با MTU کمتر از اندازه بسته روبرو شود، پیام خطای ICMP با یک 3 در نوع فیلد (destination unreachable)، یک 4 در فیلد کد (تقسیم مورد نیاز و مجموعهDF)، و اندازه بعدی MTU hop در زمینه استفاده

نشده از هدر ICMP روبرو می‌شود. پس از دریافت پیام خطای ICMP، فرستنده اصلی، MTU بسته‌ها پس از انتقال را کاهش می‌دهد.

رابط MTU

متاسفانه، اگر برخی از دستگاه‌ها در مسیر انتقال، مانند یک شبکه یا فایروال شخصی، پیام‌های ICMP را بلوک یا فیلترکنند، اثربخشی PMTUD منفی می‌گردد. اگر این یک مورد باشد، تکنیک بعدی اجتناب از تکه تکه شدن، MTU را در رابط های VPN به اندازه پایین‌تر تنظیم می‌کند. باز هم، مقدار توصیه شده 1300 بایت است. در طرح‌هایی با تونل‌های GRE، پیکربندی به رابط تونل اعمال می‌شود. بااین‌حال، در IOS سیسکو، مقدار MTUرابط تونل به‌طور پیش فرض 1514 بایت است که نمی‌توان آن را تغییر داد، بنابراین تغییر MTU IP تنها گزینه ممکن است. MTU IP را می‌توان توسط دستور ip mtu 1300 تغییر داد.

قطعه‌بندی Look Ahead

یک ویژگی که با نام قطعه‌بندی Look Ahead شناخته می‌شود (گاهی اوقات به اختصار LAF و گاهی اوقات Pre-Fragmentation نامیده می‌شود) توسط نسخه‌های فعلی IOS سیسکو پشتیبانی می‌شود. با فعال کردن قطعه‌بندی Look Ahead، روتر رمزنگاری به MTU رابط رمزنگاری خروجی توجه کرده و هدرهای رمزنگاری اضافه شده به یک بسته را ارزیابی میکند و سپس قطعات را قبل از ارسال تقسیم‌بندی‌ها به فرایند رمزگذاری در سطح IP اجرا می‌کند. هماهنگ‌کننده های رمزنگاری، رمزهای دریافت شده را به طور مستقل جدا می‌کنند و آنها را به میزبان دریافتی برای مونتاژ دوباره بسته اصلی می‌فرستند. در روترIOS سیسکو، اجرای (11) E، 12.2 T (13) یا بالاتر، به طور پیش فرض بر روی رابط‌های فیزیکی فعال است.

حداکثر اندازه بخش TCP

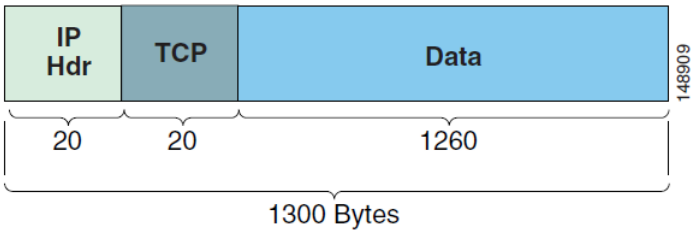
مقدار حداکثر اندازه بخشTCP (MSS) بر اندازه بسته‌های TCP تاثیر می‌گذارد. اکثریت بسته‌های داده در شبکه، TCP هستند. به غیر از ویدیو، برنامه‌های مناسب UDP (مانند DNS وNTP) متوسط بسته کمتر از 300 بایت را نمایش می‌دهند. از روتر برای نفوذ یا تنظیم MSS TCP برای جریان TCP استفاده می‌کنند به‌طوری‌که اندازه بسته داده کاهش یابد. تاثیر این مورد برای کاهش تاخیر جایی اتفاق می‌افتد که تکنیک تقسیم در لایه دوم (LFI / FRF.12) وجود نداشته باشد.

قبل از اجرای PMTUD، حداکثر اندازه بسته‌های IP برای خارج از شبکه (میزبان‌هایی که به طور مستقیم متصل نشده‌اند) 1300 بایت بود. TCP MSS تعداد بایت‌های هدر IP و TCP است، بنابراین اندازه MSS به‌طور پیش فرض 1260 بایت بود. هدر IP و TCP هرکدام 20 بایت است، بنابراین 1300 منهای 40 برابر 1260 است.

گزینه MSS تنها می‌تواند در یک بسته‌ی TCP SYN ظاهر شود و هر انتها MSS خود را اعلام کند. با اینکه مورد نیاز نیست، اغلب در هر دو جهت یکسان است. رفتار توصیه شده با معرفی PMTUD تغییییر می‌یابد، تا اجازه دهد اطلاعات بیشتر از طریق انتقال بار بیشتر در هر بسته اتفاق بیافتد. که برای داده‌ها خوب است، اما با توجه به لینک‌های نسبتا کم سرعت از اتصالات پهن باند و فقدان LFI، تاخیر سریال برای بسته‌های صوتی را معرفی می‌کند. به‌طور پیش فرض، PMTUD برای جلسات TCP که توسط روتر آغاز می‌شوند غیرفعال است. دستور ip tcp adjust-mss 1260 در دستور پیکربندی رابط Cisco IOS، مقدار گزینه MSS را برای بسته‌های TCP SYN دریافت شده از طریق آن رابط لغو می‌کند و به روتر اجازه می‌دهد که مقدار MSS ارائه شده توسط میزبان را جایگزین کند و یک جایگزین مناسب داشته باشد.

شکل 9 یک MSS را در یک بسته نشان می‌دهد.

شکل 9 شکست بسته MSS



چرا مشتریان IPsec VPN را راه اندازی می‌کنند

این بخش انگیزه‌های افراد حاضر در کسب و کار را برای مشتریانی که در حال استفاده IPsec VPN هستند، به عنوان بخشی از استراتژی WAN خود توضیح می‌دهد.

افراد حاضر در کسب و کار

تا 40 درصد از کارکنان معمولی شرکت در دفاتر شعب، دور از سایت‌های مرکزی کار می‌کنند و برنامه های کاربردی و خدمات حیاتی مورد نیاز برای عملیات تجاری را ارائه می‌دهند. همانگونه که این خدمات برای کارکنان شاخه گسترش می‌یابد، نیاز به افزایش پهنای باند برای امنیت و دسترسی بالا نیز احساس می‌شود.

به‌دلیل انعطاف‌پذیری، امنیت و هزینه بهره وری، بسیاری از مشتریان IPsec VPN را در استراتژی شرکت WAN خود به کار می‌برند. رایج‌ترین افراد حاضر در کسب و کار در بخش زیر شرح داده شده‌اند.

پهنای باند

WAN های سنتی، مانند Frame Relay و ATM، به طور معمول سرعت اتصال 128 Kbps، 256 Kbps و 512 Kbps دارند. همانطور که خدمات و برنامه‌های پیشرفته در شعبه افزایش می‌یابد، ه پهنای باند مورد نیاز نیز افزایش می‌یابد. مشتریان با دو برابر یا سه برابر شدن WAN موجود خود مواجه می‌شوند، که اغلب هزینه هنگفتی به همراه دارد، یا به دنبال گزینه‌های پهنای باند بالاتر است.

کاهش هزینه

اغلب هزینه اتصال IP با پهنای باند نسبتا بالا، مانند اتصال ISP، ارائه دهنده IP VPN، یا دسترسی به DSL / کابل پهنای باند، کمتر از مدارهای WAN موجود یا ارتقا یافته است. در نتیجه، بسیاری از مشتریان یا اتصال WAN خود را به این سرویس‌ها مهاجرت می‌دهند و یا از طریق جایگزین‌های WAN به عنوان یک مدارWAN ثانویه با سرعت بالا برای تقویت WAN خصوصی عمل می‌کنند.

خدمات شایع T1 ISP با سرعت بالا و همچنین خدمات کابل و دسترسی DSL، فشار عظیمی بر هزینه‌های خدمات سنتی WAN اعمال می‌کنند.

امنیت

مقرراتی مانند قانون بیمه درمانی و حسابدهی (HIPAA)، قانون Sarbanes-Oxley (S-Ox) و توافقنامه بازل II (در EMEA) نیاز به توصیه یا مجوز برای شرکت‌ها جهت اجرای تمام ضمانت‌های معقول برای محافظت از اطلاعات شخص، مشتری و شرکت‌های بزرگ دارند.

IPsec VPN بطور ذاتی از طریق ایجاد اعتبارات، سطح بالایی از حریم خصوصی داده‌ها را بین دستگاه‌های ارتباطی و رمزگذاری داده‌ها با استاندارد رمزگذاری اطلاعات سه بعدی (DES3) یا استاندار رمزنگاری پیشرفته (AES) فراهم می‌کنند.

مشتریان از IPsec برای رمزگذاری ارتباطات WAN خود، چه با استفاده از WAN خصوصی، IP VPN، یا اینترنت برای اتصال استفاده می‌کنند.

توسعه انعطاف‌پذیری

از آنجا که IPsec VPN را می‌توان به سرعت در هر کجا که دسترسی به اینترنت وجود دارد ایجاد کرد، درجه انعطاف‌پذیری در اتصال ادارات شعبه، حتی در مکان‌هایی که سرویس خصوصی WAN یا IP VPN ارائه نمی‌دهد متفاوت است.

حالت ارتجاعی

همانند برنامه‌های کاربردی مانند Voice over IP (VoIP)، انعطاف‌پذیری و دسترسی سطح بالا جزء نگرانی‌های اولیه هستند. مشتریان سازمانی با تکرار مدارهای اختصاصی WAN خود برای فراهم کردن سطح افزونگی مواجه هستند، که می‌تواند فوق‌العاده پرهزینه باشد.

IPsec VPN بر روی یک اتصال ISP با سرعت بالا و یا دسترسی به کابل / DSL های پهنای باند می‌تواند در اتصال ثانویه WAN برای دفاتر شعبه بسیار مفید و مقرون به صرفه باشد. بسیاری از مشتریان مسیر خود را ادامه می‌دهند تا مهمترین ترافیک در مدارهای اختصاصی WAN و مسیر پهنای باند بالاتر، ترافیک کمتر بحرانی در سراسر IPsec VPN ها به‌عنوان مسیر اتصال ثانویه مشخص شود. اگر یک خطا در مدار WAN اولیه آنها رخ دهد، IPsec VPN می‌تواند به عنوان مسیر پشتیبان ایجاد شده عمل کند.

الزامات مشتری

هنگامی که بر IPsec VPN به خاطر استراتژی اصلی یا ثانویه WAN خود تکیه می‌کنیم، مشتریان شرکت‌های سازمانی عملکرد و قابلیت اطمینان یکسانی در WAN های شخصی خود انتظار دارند. که شامل QoS، پشتیبانی چندپخشی IP و مقیاس پذیری بالا است. این بخش بسیاری از الزامات معمول مشتریان شرکت را پوشش می‌دهد.

رمزگذاری

برای اطمینان از محرمانه بودن اطلاعات منتقل شده برروی VPN، الگوریتم‌های رمزنگاری برای رمزگذاری پهنای باند بسته‌های IP استفاده می‌شوند. در زیر سه استاندارد مورد استفاده برای رمزگذاری مشترک بیان شده است:

• استاندارد رمزگذاری داده (DES)

• استاندارد سه‌گانه رمزگذاری داده (DES سه بعدی یا DES3)

• استاندارد رمزگذاری پیشرفته (AES)

DES حداقل امنیت را دارد، Triple DES جدیدتر و امن‌تر است و AES جدیدترین استاندارد و بسیار امن است. قوانین و محدودیت‌های مختلف داخلی و بین المللی از تکنولوژی رمزنگاری استفاده و آنها را صادر می‌کنند.

تمام سیستم‌عامل‌های روتر سیسکو VPN ، از جمله 870، ISR 1800، ISR 2800، ISR 3800، VXR7200 (با SA-VAM2 +)، و 7600 و یا Catalyst 6500 (با VPN SPA) از سه استاندارد رمزگذاری با شتاب سخت‌افزار پشتیبانی می‌کنند.

شتاب سخت‌افزاری رمزگذاری بنا به دو دلیل مهم است:

• توان عملیاتی در مقایسه با رمزنگاری نرم‌افزاری، به میزان قابل توجهی بهبود یافته است

• برنامه‌های کاربردی حساس به وقفه مانند VoIP، نیاز به شتاب سخت‌افزاری دارند.

تست با شتاب سخت‌افزاری نشان داده است که عملکرد انتخابی به‌طور قابل توجهی از روش رمزگذاری تاثیر نمی‌گیرد.

تأیید هویت IKE

برای اطمینان از احراز هویت جفت‌های IPsec، تبادل کلید اینترنت (IKE) استفاده می‌شود. چندین نوع احراز هویت IKE امکان‌پذیر است، از جمله دو نوع رایج آن در زیر بیان شده است:

•کلیدهای قبل از اشتراک (PSK)

• زیرساخت کلید عمومی (PKI) با استفاده از گواهینامه‌های دیجیتال X.509

برای پیاده‌سازی با تعداد کمی از شعبات، ممکن است انتخاب PSK باشد. بااین حال، همانگونه که تعداد شاخه‌ها افزایش می‌یابد، مدیریت PSK های شخصی نیز چالش‌برانگیز است و گواهینامه‌های دیجیتال X.509احتمالا گزینه بهتری هستند.

با استفاده از قابلیت Cisco IOS-CA، یک روتر سیسکو IOS می‌تواند به جای مشتریان به عنوان یک CA برای خرید یک CA شخص ثالث گرانتر یا سرویس CA مدیریت شده عمل کند. برای اطلاعات بیشتر در مورد استفاده از سیسکو IOS-CA به راهنمای صدور گواهینامه دیجیتال / PKI برای IPsec VPN مراجعه کنید.

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/DCertPKI.html

کیفیت خدمات

اگر طرح‌های IPsec VPN به‌عنوان یک جایگزین یا مکمل برای خدمات سنتی WAN پیشنهاد شوند، مشتریان انتظار دارند که همان سطح قابلیت QoS ارائه شود. IPsec VPNs و QoS در IOS سیسکو با پیاده سازی Voice and Video IPsec Enabled VPN (V3PN) یکپارچه شده‌اند.

بااین وجود، حداقل دو سطح برای QoS وجود دارد.

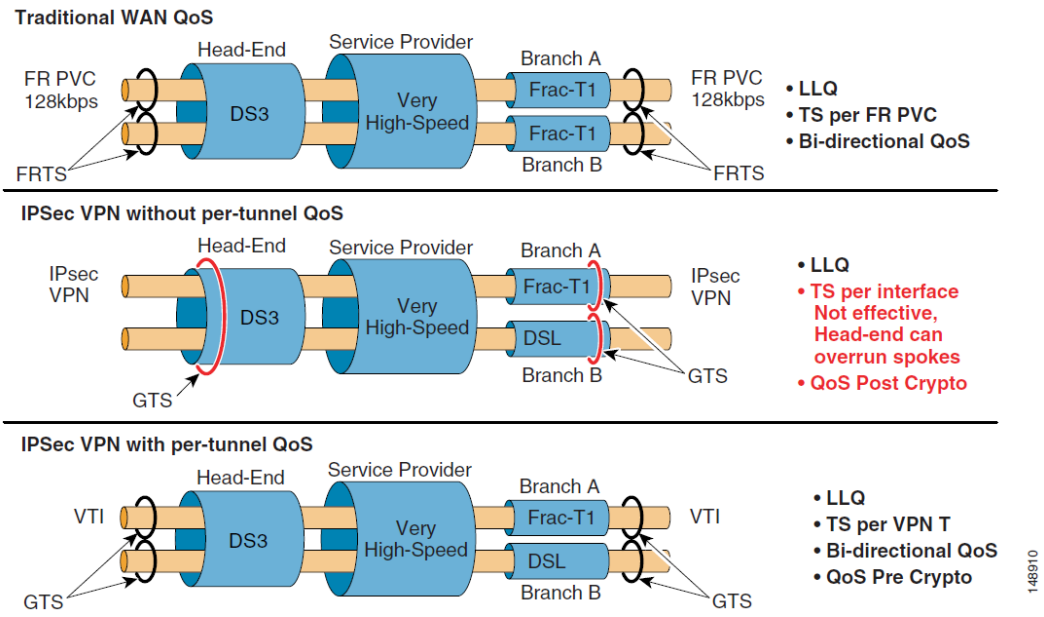
سطح رابط

QoS در کاهش سطح ترافیک در سطح رابط بسیار موثر است. به‌عنوان مثال، اگر یک دفتر با یک اتصال دسترسی T1 متصل گردد، QoS می‌تواند اطمینان حاصل کند که ترافیک از T1 تجاوز نمی‌کند و ترافیک را مهم‌تر یا حساس‌تر از VoIP اولویت‌بندی می‌کند. بیشتر بسترهای نرم‌افزاری سیسکو QoS را پشتیبانی می‌کنند، از جمله Classwise Based Queuing (CBWFQ) و شکل‌گیری ترافیک در یک سطح رابط، در غیر این صورت به عنوان صف با تاخیر کم (LLQ) شناخته شده هستند.

سطح اتصال یا جلسه

WAN های خصوصی، مانند Frame Relay، می‌توانند QoS را برای هر اتصال، مانند یک مدار مجازی (PVC)، بین فرستنده و گیرنده اجرا کنند. سیاست سرویس می‌تواند در سطح PVC برای شکل‌گیری ترافیک با سرعت هماهنگ تنظیم شود به طوری که به یک headend با سرعت بسیار بالا ایجاد کند که نمی‌تواند از کمترین سرعت از راه دور بیشتر گردد. شکل 10 این مفهوم را نشان می‌دهد.

شکل 10 مقایسه شکل‌گیری ترافیک



در مورد IPsec VPN ها، اتصال منطقی تونل بین فرستنده و گیرنده وجود دارد که دارای مشخصات پهنای باند مستقیم FR PVC نیست. علاوه براین، تونل‌های IPsec با یک سرویس QoS قابل تنظیم نیستند، بنابراین تنها گزینه اختصاص QoS در سطح رابط است. بااین‌حال، به دلیل اینکه روتر IPsec headend معمولا سرعت اتصال بالاتر از روترها دارد، برای headend ممکن است با روتر شاخه روبرو شود. این مورد در سناریوی وسط شکل 10 نشان داده شده است.

چندین گزینه برای حل این مسئله وجود دارد:

• از یک انتقال WAN استفاده کنید که یک رابط فرعی را فراهم می‌کند (مانند FR PVC) به طوریکه QoS می‌تواند اعمال شود.

• از یک ارائه‌دهنده خدماتی که خدمات QoS را در لبه ارائه‌دهنده به سمت شعبه ارائه می‌دهد، استفاده کنید.

• از دسترسی شاخه‌ای استفاده کنید که چندین بار پهنای باند downlink نسبت به پهنای باند uplink دارد، مانند 384 کیلوبیت بر ثانیه و کابل یا DSL 2 مگابیت در ثانیه.

• پیاده‌سازی QoS در تونل VPN

اگرچه پیشرفت زیادی در حال انجام است، اما هنوز هم تضمین کیفیت معادل QoS در سطح تونل چالش‌برانگیز است. P2P GRE برروی IPsec را می‌توان از طریق طراحی IPsec با اختصاص خدمات QoS در هر رابط تونل P2P GRE اجرا کرد (از جمله ترافیک عمومی). به همین ترتیب، VTI می‌تواند به صورت پویا با یک سرویس QoS مشخص شده در هر اتصال پیاده‌سازی شود. بااین‌حال، عملکرد استفاده از یک سیاست سرویس QoS با ترافیک عمومی به رابط تونل کمتر مطلوب است. بنابراین هنگامی که استفاده می‌شود، تمام بسته‌ها در پروسه تغییر قرار می‌گیرند، که باعث می‌شود CPU بالا برود.

هیچ یک از گزینه‌های طراحی QoS در هر تونل VPN در حال حاضر بسیار مقیاس‌پذیر نیستند.

برای اطلاعات بیشتر در مورد ادغام QoS و IPsec برای پشتیبانی از تاخیر/ برنامه‌های کاربردی حساس، به راهنمای طراحی Voice and Video IPsec VPN (V3PN) در URL زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND

برای اطلاعات عمومی بیشتر در مورد QoS، سرویس کیفیت خدماتSRND را ببینید. هر دو راهنما در URL زیر موجود هستند:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Bo ok.html

چندپخشی IP

چندپخشی IP یک نیاز روزافزون برای بسیاری از مشتریان سازمانی است و برخی از چالش‌ها را برای IPsec VPN ارائه می‌دهد.

ابتدا، IPsec ذاتا از انتقال بسته‌های multicast IP پشتیبانی نمی‌کند، بنابراین یک encapsulation از این ترافیک با P2P GRE یا GREچند نقطه (mGRE) مورد نیاز است. اخیرا، VTI در IOS سیسکو اجرا شده است، که IPsec را برای انتقال چندپخشی IP گسترش می‌دهد بدون اینکه نیاز به صراحت encapsulate در انتقال بسته در هدر GRE داشته باشد.

چالش دوم شامل مسئله تکرار و بسته‌های چندپخشی IP در لبه WAN شرکت می‌باشد. هر شعبه از شرکت باید یک کپی از بسته چندپخشی IP دریافت کند، به طوری که لبهWAN روتر باید بسته‌های چندپخشی IP را برای هر اتصال به شعبه‌ها تکثیر کند. سیسکو IOS برای تکثیر بسیار سریع بسته‌های چندپخشی IP بهینه‌سازی شده است.

بااین حال، هنگامی که IPsec VPN مستقر می‌شود، بین هر فرستنده یا گیرنده یک اعتماد ایجاد می‌کند و معمولا کلید رمزنگاری منحصر به فرد است. هر بسته چندپخشی IP تکثیر شده، ابتدا در هر دو سرآیند P2P GRE یا mGRE بسته‌بندی شده است و سپس توسط IPsec با کلید رمزنگاری منحصر به فرد برای هر مقصد اراسل می‌شود. رمزگذاری چنین خروجی‌های multicast IP می‌تواند در رمزگذاری روترها و سخت‌افزار شتاب دهنده VPN به منابع وابسته باشد و می‌تواند منجر به مسائلی مربوط به مقیاس‌پذیری طراحی شود.

برای کسب اطلاعات بیشتر در مورد حمایت از برنامه‌های چندرسانه‌ای IP برروی IPsec VPN، به راهنمای طراحی Multicast IP بر روی IPsec VPN در URL زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html

پروتکل‌های غیر IP

برخی از مشتریان برای انتقال پروتکل‌های غیر IP مثل IPX، برروی IPsec VPN نیازمندیهایی دارند. IPsec به طور ذاتی از انتقال بسته‌های غیر IP پشتیبانی نمی‌کند، بنابراین انحصاری از این ترافیک با P2P GRE فقط بر روی IPsec مورد نیاز است.

مسیریابی

بسیاری از شرکت‌های بزرگ WAN از پروتکل‌های مسیریابی پویای IGP مانند EIGRP و OSPF برای ارائه مسیریابی استفاده می‌کنند و حالت لینک و انعطاف‌پذیری مسیر را حفظ می‌کنند. تمام پروتکل‌های مسیریابی IGP از پخش یا IP چندپخشی به‌عنوان یک روش جدول اطلاعات مسیریابی انتقال استفاده می‌کنند.

IPsec ذاتا از انتقال بسته‌های چندپخشی IP پشتیبانی نمی‌کند، بنابراین encapsulation این ترافیک با P2P GRE، mGRE یا VTI مورد نیاز است.

کنترل از راه دور که به صورت پویا نشان داده می‌شود

خدمات WAN سنتی، مانند Frame Relay یا ATM، معمولا به آدرس‌های ایستا متکی هستند. به طور فزاینده‌ای، گزینه‌های انتقال IP مانند اتصالات ISP با سرعت بالا و به خصوص کابل پهنای باند و DSL، برای اتصال اولیه یا جایگزین WAN برای دفاتر شعبه استفاده می‌شوند.

با برخی از این انواع دسترسی، آدرس‌های ایستا ممکن است وجود نداشته باشند یا ممکن است گران‌تر باشند. بنابراین، نیاز مشتری برای طرح‌های IPsec VPN برای کار با دفاتر شعبه از طریق DHCP یا PPPoE از ارائه دهنده دسترسی در حال افزایش است.

کنترل‌های از راه دور پویای خطوط موجود، برخی از چالش‌ها را به وجود می‌آورند، زیرا هیچ نشانی ثابتی برای آن که مقصد تونل را روی روتر headend پیکربندی کنید وجود ندارد. به‌طورکلی، روترهای سربار باید با نقشه‌های رمزنگاری

پویا پیکربندی شوند و اگر روش تونل زنی یا encapsulation (مانند p2p GRE، mGRE یا VTI) استفاده شود، headends باید برای پذیرش اتصالات تونل پویا نیز پیکربندی شود.

دسترس‌پذیری بالا

اگر چه دسترس‌پذیری بالا یک موضوع وسیع است که نیاز به چندین راهنما برای طراحی مناسب دارد، ملاحظات کلیدی متعددی برای درک طراحی IPsec VPN وجود دارد. این بخش چندین فرم از دسترس پذیری بالا و رابطه آنها با IPsec VPN را بررسی می‌کند. برای کسب اطلاعات بیشتر در مورد طراحی IPsec VPN برای دسترسی و انعطاف‌پذیری بالا، V3PN را ببینید:

راهنمای طراحی کاهش بار در URL زیر:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/VPNLoad/VPN_Loadhtml

شکست Headend

نکات ذیل مربوط به شکست در طراحی IPsec VPN است که عبارتند از:

- روترهای جمع‌کننده سربار
- ماژول‌های شتاب سخت افزاری VPN (معمولا یک تیغه یا کارت اضافه)
- روترهای WAN (می‌توانند مستقل باشند یا به روترهای VPN مجتمع شوند)
- اتصالات WAN به ارائه‌دهنده سرویس (ها)

هر گونه خرابی دستگاه headend بر بخش بزرگی از اتصال تاثیر می‌گذارد. بنابراین، افزونگی باید به شدت در نظر گرفته شود. اکثر IPsec VPNهای Cisco از افزونگی برای هر نوع دستگاه، از جمله شکست کارت به کارتVPN و شکست روتر به روتر پشتیبانی می‌کنند.

یکی دیگر از خطاهای احتمالی در headend اتصال لوله با سرعت بالا (WAN) به ارائه دهنده خدمات است. باز هم، چون قطعی در این ارتباط می‌تواند بخش بزرگی از عملکرد چندگانه را تحت تاثیر قرار دهد اتصالات به ارائه‌دهندگان خدمات باید در نظر گرفته شود.

عدم موفقیت سایت

شکست یک محل از سازمان به‌طور فزاینده‌ای بخشی از الزامات طراحی مشتریان سازمانی بزرگ است. طرح‌های IPsec VPN را می‌توان به گونه‌ای طراحی کرد که سایت‌های تجمیع چند سرنشین داشته باشند که از لحاظ جغرافیایی پراکنده هستند تا سطح بالایی از انعطاف‌پذیری را در صورت شکست کامل سایت فراهم کنند.

شکست دفتر شعبه

نکات ذیل مربوط به نقص اصلی در طراحی IPsec VPN هستند:

- روترهای دفتر شعبه
- ماژول‌های شتاب‌دهنده سخت‌افزاری VPN
- اتصالات WAN به ارائه‌دهنده سرویس (ها)

هر گونه خرابی دستگاه بر قابلیت‌های محلی تاثیر می‌گذارد. بنابراین، افزونگی باید شدید در نظر گرفته شود و هزینه‌های یک قطعی برای آن شعبه محاسبه شود. باز هم بیشتر طرحهای IPsec VPN سیسکو برای هر دستگاه نوعی از کارآیی افزونگی را پشتیبانی می‌کنند، از جمله شکست کارت به کارتVPN و روتر به روتر.

یکی دیگر از شکست‌های احتمالی در شعبه، اتصال لوله به ارائه‌دهنده خدمات است. بنابراین، چون یک قطع شدن در این ارتباط می‌تواند قابلیت‌های محلی اتصالات متعدد به سرویس را تحت تأثیر قرار دهد ارائه‌دهندگان باید در نظر گرفته شوند.

شکست Statefulدر مقابل Stateless

این که آیا الزامات Stateful و یا Stateless است، در هر حالت شکست باید در نظر گرفته شود. شکست Stateless هیچ اطلاعاتی مربوط به جلسات پروتکل ترافیکی که ممکن است در زمان شکست در حال انجام باشد را حفظ نمی‌کند، درحالی‌که شکستstateful حالت ترافیک را حفظ می‌کند و تقریبا بلافاصله با بسته بعدی در جلسه ادامه می‌یابد.

عدم دسترسی به یک تونل ثانویه از طریق همگرایی پروتکل مسیریابی به طور معمول استثنا نیست و ممکن است نیاز باشد جلسات TCP / IP در حال انجام برای ارسال مجدد یا راه اندازی مجدد هستند. طرح‌های Encapsulation مستقیم IPsec همچنین می‌توانند شکست stateful، با اطلاعات مبادله شده مربوط به وضعیت جلسه IPsec بین دو headend را پشتیبانی کنند.

شکست stateful می‌تواند عملکرد را به طور معمول 1-3 ثانیه به حداقل برساند، قبل از اینکه به آن دسترسی داشته باشید روتر سرآیند آماده به کار می‌شود. شکست Stateless معمولا قبل از اینکه پروتکل مسیریابی مورد استفاده بتواند ترافیک را در مسیر جایگزین و سر و سامان دهد به 20-60 ثانیه نیاز دارد.

امنیت مجتمع

از آنجا که IPsec VPN را می‌توان اساسا در هر انتقال IP، از جمله WAN سنتی (مانند FR، ATM)، IP VPN و اینترنت مهیا کرد، خدمات امنیتی یکپارچه ممکن است نیاز مشتری باشد.

به‌عنوان مثال، اگر اینترنت به‌عنوان یک انتقال استفاده شود، ممکن است یک فایروال یکپارچه، سیستم پیشگیری از نفوذ (IPS) و سیستم‌های پیشگیری از سرویس (DoS) با یکپارچه‌سازی با طراحی IPsec VPN باشد.

یکپارچگی امنیت در ادارات شعبه بسیار بالا است و یکی از مزایای اصلی آن روتر یکپارچه خدمات سیسکو (ISR) است. در مواقع headend، عملیات امنیتی از قبل به صورت توزیع شده و یا اختصاص داده شده بود، اما توابع امنیتی یکپارچه به طور فزاینده به‌عنوان الزامات مشتری ارائه شده است.

به‌طور معمول، عملکردهای امنیتی مانند عملیات محاسباتی فایروال نسبتا شدید هستند، بنابراین اگر مسیریاب همان VPN را فراهم کند، باید برروی روترهای headend یا branch office و سایر خدمات امنیتی تاثیر بگذارد.

مشبک کردن پویا

طراحی معمولی یک WAN خصوصی سنتی همانند طرح‌های IPsec VPN که عمدتا مستقر هستند، توپولوژی hub-and-spoke است. ادارات شعبه دارای اتصال به یک یا چند سربرگ VPN هاب‌ها هستند.

برخی از مشتریان شرکت ممکن است برای ارتباط مستقیم بین دفاتر شعبه الزاماتی داشته باشند و اگر این الزامات به اندازه کافی قابل توجه باشند، مشتریان ممکن است نیاز به مشبک‌سازی بیشتری در توپولوژی طراحی IPsec VPN داشته باشند.

اگر اتصال مستقیم شاخه به شاخه برای چند شعبه بزرگ در توپولوژی شناخته شده باشد، اتصالات اضافی IPsec VPN را می‌توان در طراحی بین این سایت‌ها از پیش تعیین کرد.

اگر مشتری برای دفاتر شعبه نیاز به اتصال پویا به دیگر شعبه‌ها داشته باشد، روترهای سیسکو VPN و سیسکو IOS می‌توانند این قابلیت را ارائه دهند. تأثیرات توپولوژی WAN باید در صورت اجرای یک توپولوژی مورد توجه قرار گیرد.

مقیاس‌پذیری

انعطاف‌پذیری IPsec VPN منجر به انتظارات مشتری از نقاط جمع شدن در مقیاس بزرگتر نسبت به WAN های خصوصی می‌شود. به طوری که شبکه‌های WAN روت شده به طور معمول برای جمع‌آوری تقریبا 200 PVC طراحی شده‌اند، مشتریان انتظار دارند که در مجموع 500، 1000 یا حتی 5000 از اتصالات تونل IPsec VPN را در یک یا چند مکان hub جمع کنند.

بسیاری از عوامل موثر بر مقیاس‌پذیری یک طراحی IPsec VPsp، شامل دسترسی به سرعت اتصال، محدودیت‌های مسیریابی peer، توان عملیاتی رمزگذاری IPsec و ختم تونل IPsec هستند. چگونه مقیاس بزرگی را داشته باشیم

در حالی که حفظ عملکرد و در دسترس بودن آن به چالش کشیده شده است و نیاز به مراقبت برنامه‌ریزی و طراحی دارد.

مقیاس‌بندی طراحی، صفحه 41، را برای توضیح کامل در مورد مقیاس‌پذیری برای IPsec VPN مشاهده کنید.

تامین و مدیریت

به دلیل انعطاف‌پذیری IPsec VPN، بسیاری از مشتریان سازمانی انتظار دارند که این شبکه‌ها را برای تعداد نسبتا زیادی از دفاتر شعبه مستقر کنند. این مسئله می‌تواند چالش‌هایی را برای تامین و مدیریت به همراه داشته باشد.

درک تکنولوژی

بیشتر کارکنان شبکه WAN با مسیریابی و تکنولوژی‌های خصوصی شبکه WAN آشنا هستند. بسیاری QoS را تجربه کرده‌اند. بااین‌حال IPsec از لحاظ تاریخی فن آوری دسترسی امن و از راه دور بوده است و به احتمال زیاد توسط کارکنان شبکه امنیت مدیریت شده است، که ممکن است با فن‌آوری‌های WAN و مسیریابی آشنا نباشند.

به‌طورمشابه، WAN های خصوصی به‌طورکلی یک رسانه معتبر محسوب می‌شوند، درحالی‌که IPsec VPN ها اغلب در رسانه‌های غیرقابل اعتماد مانند اینترنت مستقر هستند. کارکنان شبکه WAN ممکن است تجربه زیادی در مورد مسائل امنیتی نداشته باشند و ممکن است کارمندان InfoSec نیاز به شرکت فرایند طراحی داشته باشند.

این مسئله می‌تواند یک چالش در این شرکت برای کارکنان شبکه مشتری ایجاد کند زیرا آن‌ها باید تعدادی از فن‌آوری‌های محرمانه را برای پیاده‌سازی IPsec VPN به‌عنوان استراتژی WAN درک کنند. ساده‌سازی برنامه‌ریزی، طراحی و استقرار باید یک هدف اولیه باشد.

دسترسی بدون تماس

مشتریان سازمانی مایل به پیکربندی روترهای تجمع یافته سرآیند VPN خود برای دسترسی بدون تماس در دفاتر شعبه جدید هستند. در حالت ایده آل، مشتریان می‌خواهند روتر headend را یک بار پیکربندی کنند و سپس لازم نباشد تا خطوط پیکربندی جدیدی را برای تأسیس شعبه‌های جدید ایجاد کنند که عملکرد عملیات روترهای VPN را ا مختل کند.

برای ارائه دسترسی بدون تماس، روترهای سربار باید با نقشه‌های رمزنگاری پویا یا پروفایل‌ها و تونل زنی پویا (مانند تنظیمات mGRE یا VTI) پیکربندی شوند، به‌طوری‌که اتصالات جدید را بتوان بدون تغییر مسیر روتر headend ایجاد کرد.

سیسکو چند گزینه طراحی بدون تماس را فراهم می‌کند، که در انتخاب طراحی، صفحه 25 توضیح داده شده است.

مدیریت در حال اجرا

مشتریان سازمانی ممکن است ابزار و سیستم‌های مدیریتی خاص خود را داشته باشند یا ممکن است مایل باشند یک سیستم مدیریتی خاص برای VPN IPsec مستقر کنند. در صورت تمایل، سیسکو تعدادی از ابزارهای مدیریتی لازم برای این منظور را ارائه می‌دهد، که شامل موارد زیر است:

- سیستم مدیریتی VPN (VMS)
- مرکز راه‌حل‌های IP (ISC)

توصیف بیشتر در مورد محصولات مدیریت شبکه خارج از محدوده این طرح برای طراحی است.

ارائه‌کننده خدمات

VPN ها ذاتا به یک یا چند ارائه‌دهنده خدمات متکی هستند تا خدمات دسترسی به headend و شعبه‌ها را برای راه‌اندازی شبکه ارائه دهند. انتخاب یک ارائه‌دهنده خدمات یک عنصر مهم در استقرار یک IPsec VPN است.

عوامل در نظر گرفته شده شامل هزینه، خدمات در دسترس، قابلیت اطمینان جغرافیایی مورد انتظار در پوشش VPN مشتری است. بنابراین شرکت حداقل باید SLA با ارائه دهنده سرویس داشته باشد تا عناصر حیاتی سرویس VPN خود را مشخص کند. این عوامل شامل دسترسی، پهنای باند و تأخیر است.

موقعیت‌هایی که نیاز به یک شرکت برای استفاده از ارائه‌دهندگان خدمات مختلف برای پوشش مکان‌های شعبه خود دارند یک سطح از پیچیدگی را اضافه می‌کنند و می‌تواند به طور بالقوه برای دستیابی به سطح مورد نظر از سرویس VPN پایان به پایان تلاش کنند. به همین دلیل، سیسکو یک SLA با یک سرویس‌دهنده واحد توصیه می‌کند که می‌تواند سطح خدمات پایان به پایان برای مکان‌های سازمانی را تضمین کند.

همچنین برخی از ارائه‌دهندگان خدمات اینترنتی برای خدمات DSL و کابلی، قوانین انتقال برای سرویس اضافی را پیاده‌سازی می‌کنند. این مسئله به این معنی است که پروتکل‌هایی مانند IPsec ممکن است مسدود شوند مگر اینکه مشتری در خدمات کلاس کسب و کار اشتراک داشته باشد.

انتخاب طراحی

این بخش به بررسی سطح بالای چندین توپولوژی طراحی IPsec VPN می‌پردازد که در حال حاضر مستقر هستند. مزایا و معایب برای هر یک ارائه می‌شود. پس از آن در بخش بعدی نقشه‌های مورد نیاز مشتری برای انتخاب مناسب‌ترین طراحی توصیه می‌شود.

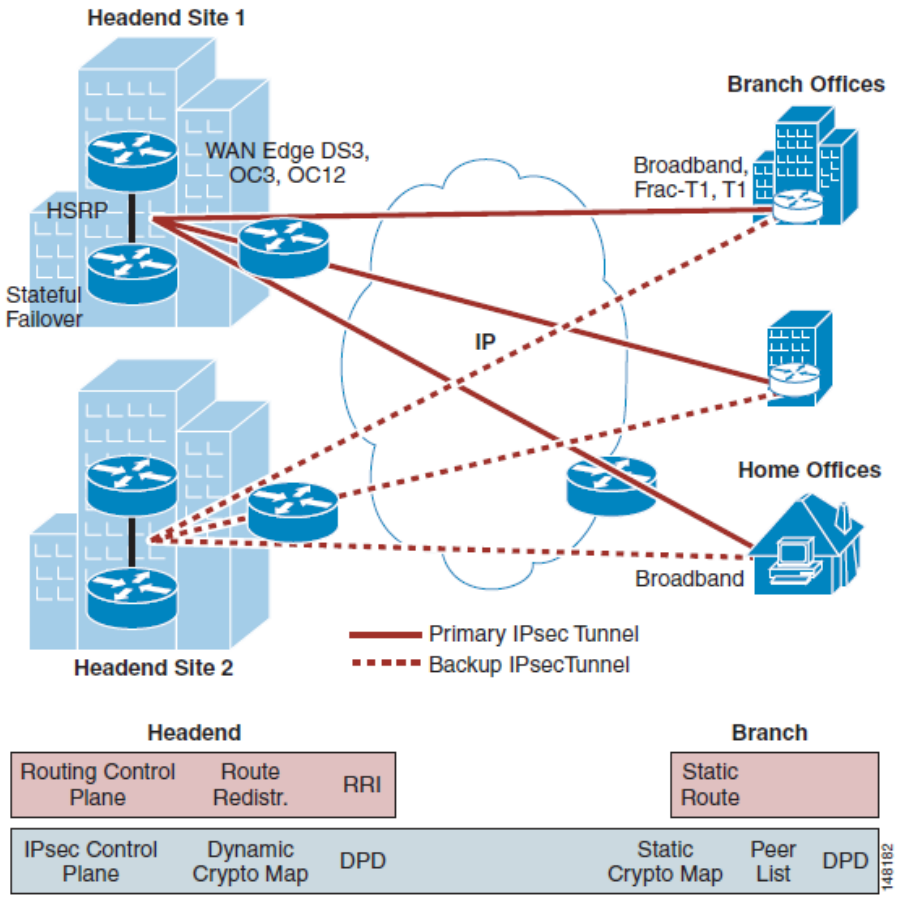
طراحی Encapsulation مستقیم IPsec

خود IPsec حالت عملیاتی تونلی را فراهم می‌کند که می‌تواند به عنوان یک روش اتصال مستقل مورد استفاده قرار گیرد. این گزینه اصلی‌ترین مدل طراحی IPsec VPN است. طرح‌های IPsec Direct Encapsulation نمی‌توانند پروتکل‌های مسیریابی پویا IGP یا ترافیک IPmc را حمل کنند.

بررسی اجمالی طراحی

شکل 11، طراحی IPsec Direct Encapsulation را نشان می‌دهد.

شکل 11 طراحی IPsec Direct Encapsulation



هر یک از سایت‌های از راه دور یک تونل IPsec را به یک headend pre-defined تعریف می‌کند. کنترل از راه دور می‌تواند آدرس‌های IP ایستا یا پویا داشته باشد، درحالی‌که headendها باید آدرس‌های IP ثابت داشته باشند. قابلیت اطمینان توسط IPsec Stateful Failover در مکان‌های headend ارائه می‌شود. روترهای شاخه می‌توانند با یک لیست از سرفصلها پیکربندی شده باشند. اگر اتصال با اولین headend ایجاد نشد، Headend های بعدی تا زمانی که ارتباط موفق ایجاد شود تلاش می‌کنند.

نقشه‌های رمزنگاری پویا را می‌توان بر روی روترهای headend پیکربندی کرد، مثلا اتصالات تونل ورودی جدید را می‌توان بدون نیاز به ایجاد دستی تونل جدید در روتر headend ایجاد کرد.(Dead Peer Detection (DPD

برای شناسایی از دست دادن یک اتصال peer فعال است و تزریق مسیر معکوس (RRI) در headend پیکربندی می‌شود تا مسیرها برای زیر شبکه‌های روتر شاخه در جدول مسیریابی مشخص شوند. هیچ پروتکل مسیریابی بین روترهای headend و شاخه مبادله نمی‌شود.

مزایا

طرح‌های Encapsulation مستقیم IPsec مزایای زیر را ارائه می‌دهند:

• تنظیمات نسبتا ساده است

• تمام پلتفرم‌های روتر سیسکو IOS این طراحی را پشتیبانی می‌کند، از جمله 870، 1800/2800/3800 ISR، VXR7200 و 7600. همچنین سیستم عامل PIX، ASA و VPN3K نیز پشتیبانی می‌کنند.

• نقشه‌های رمزنگاری پویا را می‌توان بر روی روترهای headend مانند این تونل ورودی پیکربندی کرد و اتصالات را می‌توان بدون نیاز به تنظیم دستی در هر تونل جدید در روتر headend ارائه کرد.

• قابلیت همکاری با دستگاه‌های همکار غیرسیسکو وجود دارد که سازگار با RFC هستند.

• جفت‌های مسیریابی IGP محدودیت مقیاس‌پذیری ندارند، زیرا هیچ پروتکل مسیریابی IGP پویایی بر روی تونل اجرا نمی‌شود.

معایب

طرح‌های Encapsulation مستقیم IPsec معایبی را ارائه می‌دهد:

• از چندپخشی IP یا پروتکل‌های غیر IP (چند پروتکلی) پشتیبانی نمی‌کنند.

• از پروتکل‌های مسیریابی IGP بر روی تونل VPN پشتیبانی نمی‌کنند.

• اگر تونل اولیه از دست رفته باشد، هیچ تونل ثانویه‌ای از پیش تعیین نشده است، بنابراین تونل جدید باید قبل از اینکه ترافیک ادامه یابد، به headend متصل شود.

• توزیع تونل IPsec به روتر headend می‌تواند غیرقطعی باشد، زیرا از دست دادن نتایج اتصال در روترهای از راه دور یک تونل به جفت‌های بعدی ایجاد می‌کنند. به‌عنوان مثال، کنترلرها بعد از بهبود خرابی به‌طور خودکار به headend اولیه خود متصل نمی‌شوند.

• امکان اجرای یک سرویس QoS در هر تونل VPN وجود ندارد.

• زمانی که خط مشی سرویس QoS با طراحی IPsec پیکربندی شده است، تعامل بین IPsec و QoS می‌تواند بسته ضد پاسخ به IPsec باشد.

بیشترین استفاده معمول

طرح‌های Encapsulation مستقیم IPsec معمولا زمانی استفاده می‌شوند که نیازی به مسیریابی پویا IGP یا چندپخشی IP وجود ندارد و ادارات شعبه دارای چندین زیرساخت و یا یک زیرساخت واحد مانند کارگران دورافتاده و اداره کوچک (SOHO) هستند. طرح‌های Encapsulation مستقیم IPsec معمولا نیز در برنامه‌های دسترسی از راه دور استفاده می‌شوند، جایی که یک دستگاه واحد (مانند یک لپ تاپ) یک تونل را از طریق یک مشتری آغاز می‌کند.

برای کسب اطلاعات بیشتر در مورد استفاده از طرح‌های Encapsulation مستقیم IPsec برای اتصال WAN، به راهنمای طراحی Encapsulation مستقیم IPsec در URL زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap..html

Point-to-Point GRE در طراحی IPsec

IPsec را می‌توان در رابطه با p2p GRE (یک تونل GRE نقطه به نقطه رمزگذاری شده IPsec) برای ارائه قابلیت‌های اضافی به کار برد. با اضافه کردن P2P GRE به IPsec، پروتکل‌های مسیریابی پویا IGP و ترافیک چندپخشی IP را می‌توان از طریق تونل VPN حمل کرد.

معماری Headend- یک Headend واحد در مقابل Headend دوگانه

هنگام اجرای P2P GRE بر روی طراحی IPsec، دو معماری سربار زیر می‌تواند در سایت مرکزی اجرا شود:

- تک لایه
- سطح دوگانه

معماری Headend تک لایه

در یک معماری Headend تک لایه، P2P GRE و Crypto به صورت کاربردی و هماهنگ در CPU روترهای یکسان وجود دارد. سرویس روترهای Headend چندین p2p GRE را بر روی تونل‌های IPsec برای تعداد معینی از سرویس‌ها ارائه می‌دهند. علاوه بر این، برای پایان دادن به تونل VPN در سایت مرکزی، روتر headend را می‌توان در مسیرهای شعبه با استفاده از پروتکل های مسیریابی IP (EIGRP، OSPF و غیره) تبلیغ نمود.

معماری Headend دوگانه

در یک معماری headend دوگانه، P2P GRE و رمزنگاری به صورت کاربردی و هماهنگ در CPU روترهای یکسان وجود دارد. روترهای P2P GRE و همچنین روترهای Crypto وجود دارند و با p2p GRE بر روی تونل IPsec و برای تعداد معینی از محل شعبه‌ها ارائه می‌شوند. بعلاوه برای توقف تونل VPN در سایت مرکزی، روترهای p2p GRE می‌توانند مسیرهای شاخه‌ای را با استفاده از پروتکل‌های مسیریابی IP (EIGRP، OSPF، و غیره) تبلیغ کنند.

عملکرد و ارزش

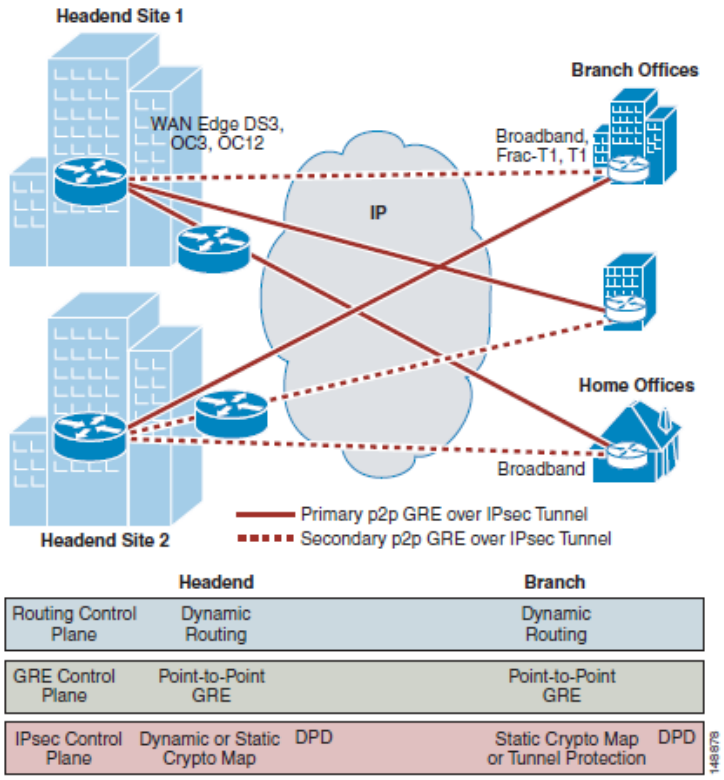
با توجه به عملکرد و ارزش، این دو باید با هم در نظر گرفته شوند. عملکرد براساس تعداد بسته‌های یک پلت‌فرم است که می‌تواند در یک فریم زمان مشخص منتقل شود یا بسته‌ها در هر ثانیه (pps) است. ارزش، قیمت یک پلت‌فرم خاص براساس نرخ PPS است. برای کسب اطلاعات بیشتر هنگام انتخاب یک معماری سرآیند تک سطحی در مقابل معماری سرآید دوگانه، به راهنمای طراحی GRE Point-to-Point بر روی IPsec مراجعه کنید که در آدرس زیر آمده است:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_GRE_IPSec.html IPSec/P2P

بررسی اجمالی طراحی

شکل P2P GRE 12 را بر روی طراحی IPsec نشان می‌دهد.

شکل P2P GRE 12 در طراحی IPsec



هر سایت از راه دور با GRE P2P بر روی تونل IPsec به یک headend از پیش تعریف شده متصل می‌شود. که می‌تواند آدرس IP های ایستا یا پویا داشته باشد، درحالی‌که headends باید آدرس‌های IP ثابت داشته باشند.

قابلیت اطمینان را می‌توان با P2P GRE از طریق تونل IPsec بر روی روترهای چندگانه header در یک یا چند موقعیت مکانی جغرافیایی پیکربندی کرد. یک پروتکل مسیریابی پویا IGP بر روی P2P GRE و تونل IPsec مبادله می‌شود و تونل‌های اولیه / ثانویه با معیارهای متفاوتی پیکربندی می‌شود.

DPD را می‌توان برای شناسایی از دست دادن اتصال peer فعال کرد.

مزایا

طرح‌های P2P GRE بر روی IPsec مزایای زیر را ارائه می‌دهد:

• پروتکل‌های چندپخشی IP و غیر IP پشتیبانی می‌شوند.

• پروتکل‌های مسیریابی پویا IGP بر روی تونل VPN پشتیبانی می‌شوند.

• از تمامی پلتفرم‌های روتر سیسکو IOS پشتیبانی می‌شود.

• سیاست های سرویس QoS را می‌توان در هر p2p GRE بر روی تونل IPsec پیکربندی کرد (مقیاس پذیری ممکن است یک مسئله باشد).

• توزیع تونل IPsec بر روی روترهای headend، با متریک‌های مسیریابی و همگرایی انتخاب بهترین مسیر قطعی است.

• تمام پشتیبان‌های پویای اولیه و ثانویه p2p GRE بر روی تونل IPsec از پیش تعیین شده است، به‌طوری‌که لازم نیست تونل جدید در صورت وقوع شکست در یک سناریو، ایجاد شود.

معایب

P2P GRE بر روی طرح‌های IPsec دارای معایب زیر است:

• پیکربندی هر رابط تونل P2P GRE استاتیک است و می‌تواند به headend طولانی پیکربندی منجر شود.

• تأمین دفاتر شعبه‌های جدید به‌طور معمول نیازمند یک تغییر پیکربندی / علاوه بر روتر (های) headend است.

• جفت‌های مسیریابی IGP تمایل دارند مقیاس‌پذیری را بیش از طرح‌های Encapsulation مستقیم IPsec محدود کنند.

• سیاست‌های سرویس QoS در هر تونل به دلیل ترافیک عمومی موجود در مقیاس پذیری محدودیت دارند.

• زمانی که خط مشی سرویس QoS با طراحی IPsec پیکربندی شده باشد، تعامل بین IPsec و QoS می‌تواند منجر به بسته ضد پاسخ IPsec شود.

بیشترین استفاده معمول

P2P GRE بر روی IPsec designs معمولا زمانی استفاده می‌شود که نیازمندی‌هایی برای مسیریابی و / یا IPmc وجود داشته باشد. آنها همچنین در شرایطی هستند که دفاتر شعبه دارای چندین زیرشبکه است که برای تبادل پروتکل‌های مسیریابی پویا IGP مطلوب هستند.

برای کسب اطلاعات بیشتر در مورد استفاده از P2P GRE بر روی طرح های IPsec برای اتصالات شرکت WAN، به Point-to-Point GRE بر روی راهنمای طراحی IPsec در آدرس زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2GRE_IPSec.html

VPNپویای چندنقطه‌ای- طراحی تکنولوژی Hub-and-Speoke

DMVPN، پروتکل‌های IPsec، mGRE و NHRP را ترکیب می‌کند. DMVPN دو حالت از عملیات را دنبال می‌کند:

نقطه به نقطه GRE از طریق طراحی IPsec

• توابع طراحی و توزیع توپولوژی DMVPN - بسیار مشابه با P2P GRE بر روی طراحی IPsec است و تمام تونل‌ها بین روترهای Headend و دور قرار دارند.

• طراحی توپولوژی DMVPN spoke-to-spoke- علاوه بر توپولوژی DMVPN Hub-and-Speoke این قابلیت برای ایجاد تونلهای دونفره برای ارتباطات مستقیم نیز امکان‌پذیر است.

این بخش عملیات طراحی توپولوژی DMVPN را بررسی می‌کند. VPN پویا چندنقطه‌ای- طراحی توپولوژی Speoke-to-Speake ، صفحه 34 نحوه طراحی عملیات توپولوژی DMVPN را بررسی می‌کند.

معماری Headend-Headend تک لایه در مقابل Headend دوگانه

هنگام اجرای یک طرح توپولوژی DMU و Hub ، دو معماری headend زیر می‌تواند در سایت مرکزی اجرا شود:

• تک لایه

• سطح دوگانه

معماری headend تک لایه

در معماری headend تک لایه، mGRE و رمزگذاری، عملکردی مشابه برCPU روتر یکسان دارند. روترهای Headend تونل‌های متعددی از DMVPN را برای یک تعداد مجاز از مکان شعبه‌ها سرویس می‌دهند. علاوه بر پایان دادن به تونل VPN در سایت مرکزی، روترهای سربار می‌توانند تبلیغ کننده مسیرهای شعبه با استفاده از پروتکل‌های مسیریابی IP (EIGRP، OSPF و غیره) باشند.

معماری headend دوگانه

در معماری headend دوگانه، mGRE و رمزنگاری عملکردی مشابه CPU روترهای یکسان دارند. روترهایmGRE وجود دارند و برای تعدادی از مکان‌های دفتر شعبه عمل می‌کنند. علاوه بر پایان دادن به تونل VPN در سایت مرکزی، روترهای headend mGRE می‌توانند مسیرهای شعبه را با استفاده از IP تبلیغ کننده پروتکل‌های مسیریابی (EIGRP، OSPF، و غیره) بیایند.

عملکرد و ارزش

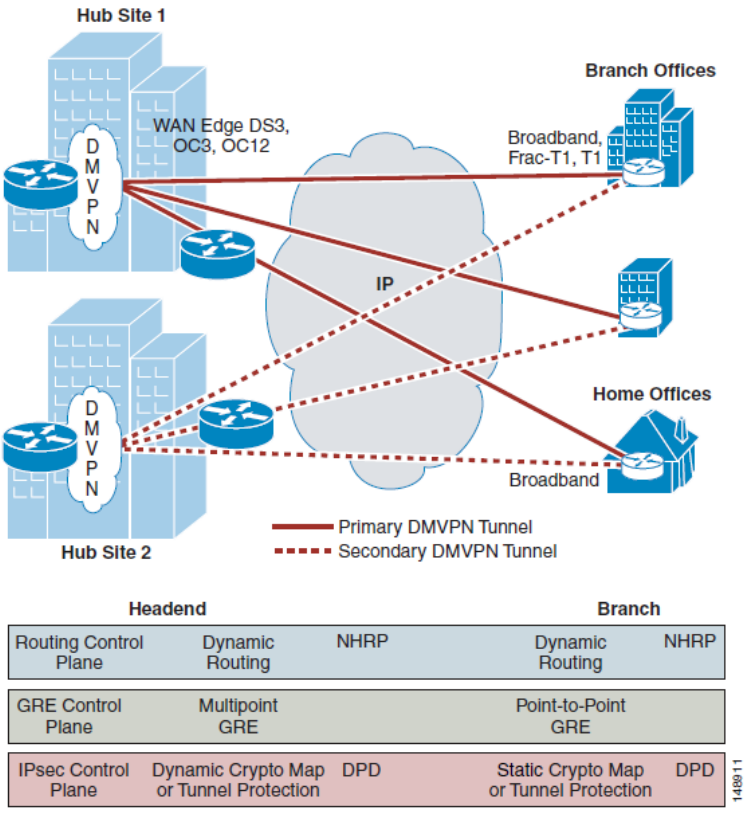
با توجه به عملکرد و ارزش، این دو باید با هم در نظر گرفته شوند. عملکرد، براساس pps یک پلت‌فرم می‌تواند در یک فریم زمانی مشخص منتقل شود. ارزش، قیمت یک پلت‌فرم خاص براساس نرخ pps است. برای کسب اطلاعات بیشتر هنگام انتخاب یک معماری Headend تک لایه در مقابل معماری Headend دوگانه، به راهنمای طراحی دینامیک چند نقطه‌ای VPN (DMVPN) در آدرس زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html

بررسی اجمالی طراحی

شکل 13، طرح توپولوژی DMVPN را برای hub-and-spoke نشان می‌دهد.

شکل 13 طراحی توپولوژی DMVPN برای hub-and-spoke



هر یک از سایت‌های راه دور با یک رابط تونل P2P GRE به یک headend pre-defined تعریف شده است. روتر(های) headend از رابط‌های mGRE استفاده می‌کنند تا به صورت پویا اتصالات تونلی جدید را بپذیرند.

قابلیت تسریع با تطبیق تونل‌های DMVPN بر روی رابط mGRE بر روی چندین روتر headend در یک یا چند مکان جغرافیایی hub ارائه می‌شود.

ریموت‌ها می‌توانند IP های ایستا یا پویا داشته باشند، درحالی‌که headend ها باید آدرس‌های IP ثابت داشته باشند.

پروتکل مسیریابی پویا IGP بر روی تونل‌های DMVPN مبادله می‌شود و تونل‌های اولیه / ثانویه با پیکربندی معیارهای مسیریابی کمی متفاوت هستند.

حفاظت از تونل IPsec به‌طورکلی برای نشان دادن ویژگی‌های رمزنگاری به تونلی که توسط آن ایجاد می‌شود استفاده می‌شود. DPD را می‌توان برای شناسایی از دست دادن اتصال peer فعال کرد.

NHRP بر روی هر دو روتر headend و branch office پیکربندی شده و برای استفاده از رابط‌های mGRE مورد نیاز است.

مزایا

طرح‌های توپولوژی DMVPN دارای مزایای زیر می‌باشند:

- چندپخشی IP پشتیبانی می‌شود.
- پروتکل‌های مسیریابی پویا IGP بر روی تونل VPN پشتیبانی می‌شوند.
- از تمام سیستم‌عامل‌های روتر سیسکو IOS پشتیبانی می‌شود (برخی محدودیت‌ها در سیستم‌عامل‌های روتر بالا-پایان وجود دارد).
- توزیع تونل IPsec به روتر headend، با متریک‌های مسیریابی و همگرایی انتخاب بهترین مسیر قطعی است.
- تمام تونل‌های DMVPN اولیه و ثانویه / پشتیبان از قبل ساخته شده‌اند، به‌طوری‌که یک تونل جدید در صورت وقوع یک سناریوی شکست، نباید ایجاد شود.

• پیکربندی هر دوی IPsec و mGRE، با پیکربندی ساده پویا است. تأمین دفاتر جدید شعبه را می‌توان بدون پیکربندی تغییر / اضافه کردن به روتر headend (ها) انجام داد.

معایب

طرح‌های توپولوژی DMVPN دارای اختلافات زیر هستند:

• عدم پشتیبانی از پروتکل‌های غیر IP.

• جفت‌های مسیریابی IGP تمایل دارند مقیاس‌پذیری طراحی را محدود کنند.

• عدم قابلیت همکاری با روترهای غیرسیسکو IOS.

• برخی از پیچیدگی‌های اضافه شده با DMVPN نیاز به پیکربندی NHRP و همچنین اضافه شدن پیچیدگی در عیب‌یابی دارند.

• امکان اجرای یک سیاست سرویس QoS در هر تونل VPN امکان‌پذیر نیست.

• زمانی که خط مشی سرویس QoS با طراحی IPsec پیکربندی شده باشد، تعامل بین IPsec و QoS می‌تواند موجب بسته IPsec ضد پاسخ گردد.

• پشتیبانی شتاب مستقیم برای اضافه کردن کلید اضافی تونل 4 بایت mGRE در روتر بالا-پایان وجود ندارد، مانند سیسکو 7600 (یا سیسکو کاتالیست 6500) با یک VPNSM یا VPN SPA. بااین حال، یک کار وجود دارد که برخی از قابلیت‌های شتاب را در خود دارد (برای اطلاعات بیشتر به مقیاس طراحی، صفحه 41 نگاه کنید).

بیشترین استفاده معمول

طرح‌های توپولوژی DMVPN معمولا برای مسیریابی و / یا چندپخشی IP موجود برای IGP مورد استفاده قرار می‌گیرند. آنها همچنین در شرایطی که دفاتر شعبه چندگانه هستند استفاده می‌شود زیرا subnet ها برای تبادل پروتکل‌های مسیریابی پویا IGP مطلوب هستند.

علاوه براین، به دلیل تنظیمات ساده‌تر و فراهم آوردن امکانات بی‌نظیر شعبه‌های جدید، یک طراحی توپولوژیک و توزیع شده DMVPN برای تنظیمات headend بر یک رویکرد تونل P2P GRE ترجیح داده می‌شود. حتی در مواردی که پیکربندی GRE static P2P در روترهای شاخه استفاده می‌شود، استفاده از mGRE در headends مفید است.

در نهایت، طرح‌های توپولوژی DMU و Hub و spoke به‌عنوان اولین قدم به سوی طراحی توپولوژی DMVPN بحث می‌شوند (به بخش‌های بعدی نگاه کنید).

برای کسب اطلاعات بیشتر در مورد استفاده از طرح‌های توپولوژی DMUVN و DMVPN برای اتصال WAN، راهنمای طراحی VPN (DMVPN) WAN چندین نقطه را در URL زیر مشاهده کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html.

VPN چندنقطه پویا – طراحی توپولوژی Spoke-to-Spoke

DMVPN ها همچنین می‌توانند در یک طراحی توپولوژیک Spoke-to-Spoke، که در آن روترهای شعبه می‌توانند به صورت پویا ارتباطات تونل DMVPN را بین یکدیگر برقرار کنند، پیکربندی شوند.

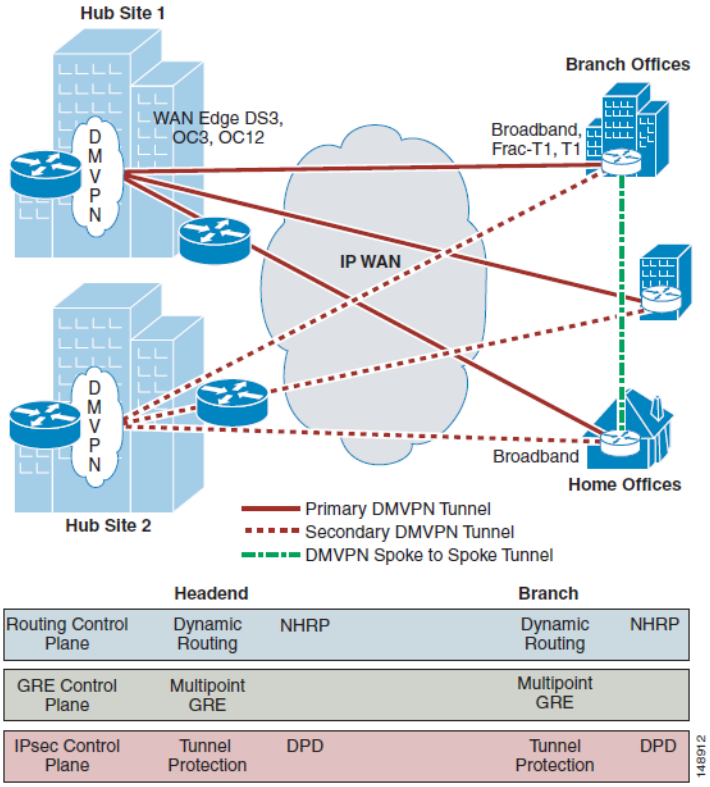
یک طراحی توپولوژیکhub-and-Spoke DMVPN همیشه به‌عنوان یک پیش شرط برای صحبت کردن با طراحی توپولوژی DMVPN وجود دارد، به این معنی که دفاتر شعب همیشه یک اتصال تونل DMVPN دارند که به روتر headsend اختصاص داده شده است.

با طراحی توپولوژی Spoke-to-Spoke DMVPN، هر روتر دفتر شعبه با یک یا چند رابط mGRE پیکربندی می‌شود.

بررسی اجمالی طراحی

شکل 14، طراحی توپولوژی Spoke-to-Spoke DMVPN را نشان می‌دهد.

شکل 14 طراحی توپولوژی Spoke-to-Spoke DMVPN



هر سایت از راه دور با یک تونل DMVPN به یک headend از پیش تعریف شده متصل می‌شود. روتر headend (ها) از رابط‌های mGRE استفاده می‌کنند تا به طور پویا اتصالات تونل جدید را بپذیرید.

قابلیت تسریع با تطبیق تونل‌های DMVPN به رابط mGRE بر روی چندین روتر headend در یک یا چند مکان جغرافیایی hub ارائه می‌شود.

ریموت‌ها می توانند IP های ایستا یا پویا داشته باشند، درحالی‌که headends باید آدرس‌های IP ثابت داشته باشند.

یک پروتکل مسیریابی پویا IGP تنها در مورد تونل‌هایDMVPN hub-and0spoke مبادله می‌شود و تونل‌های اولیه / ثانویه با پیکربندی معیارهای مسیریابی کمی متفاوت هستند. هیچ اطلاعات مسیریابی بین spokeها رد و بدل نمی‌شود.

IPsec Tunnel Protection به‌طورکلی برای نشان دادن ویژگی‌های رمزنگاری به تونل‌ها استفاده می‌شود. DPD را می‌توان برای تشخیص از دست دادن اتصال NHRP بر روی پیکربندی هر دو روتر headend و branch office فعال کرد و برای استفاده از رابط mGRE، افزودن mGRE در روترهای راه دور مورد نیاز است.

مزایا

طرح‌های توپولوژی DMVPN مزایای زیر را ارائه می‌دهند:

• چندپخشی IP فقط در تونلهای hub-and-spoke پشتیبانی می‌شوند (نه به طور مستقیم بین spoke ها).

• پروتکل‌های مسیریابی پویا IGP بر روی تونل VPN hub-and-spoke پشتیبانی می‌شوند (اما بین spokeها مبادله نمی‌شوند).

• از تمام سیستم‌عامل‌های روتر سیسکو IOS پشتیبانی می‌کنند (برخی محدودیت‌ها در سیستم‌عامل‌های روتر بالا-پایان وجود دارد).

• توزیع تونل IPsec به روتر headend، با متریک‌های مسیریابی و همگرایی انتخاب بهترین مسیر قطعی است.

• تمام تونل‌های DMVPN اولیه و ثانویه / پشتیبان از قبل ساخته شده‌اند، به طوری‌که یک تونل جدید در صورت وقوع یک سناریوی شکست، نباید ایجاد شود.

• پیکربندی هر دوی IPsec و mGRE، با پیکربندی ساده پویا است. تأمین دفاتر جدید شعبه را می‌توان بدون پیکربندی تغییر / اضافه کردن به روتر headend (ها) انجام داد.

معایب

طرح‌های توپولوژی spoke-to-spoke DMVPN دارای معایب زیر هستند:

• عدم پشتیبانی از پروتکل‌های غیر IP.

• هیچ QoS بین روترهای spoke برای تونلهای spoke-to-spoke وجود ندارد و این باعث می‌شود که مقصد روتر با ترافیک روبرو شود. در نتیجه، برنامه‌های کاربردی حساس به تاخیر / jitter / drop-sensitive از قبیل VoIP و Video over IP، "بهترین تلاش" برای توپولوژی spoke-to-spoke هستند.

• جفت‌های مسیریابی IGP تمایل دارند مقیاس‌پذیری طراحی را محدود کنند.

• عدم قابلیت همکاری با روترهای غیرسیسکو IOS.

• برخی از پیچیدگی‌های اضافه شده با DMVPN نیاز به پیکربندی NHRP، و همچنین اضافه شدن پیچیدگی در عیب‌یابی دارند.

• امکان اجرای یک سیاست سرویس QoS در هر تونل VPN امکان‌پذیر نیست.

• هنگامی که خط مشی سرویس QoS با طراحی IPsec پیکربندی شده باشد، تعامل بین IPsec و QoS می‌تواند بسته ضدپاسخ باشد.

• پشتیبانی شتاب مستقیم برای اضافه کردن کلید اضافی تونل 4 بایت mGRE در روتر بالا-پایان وجود ندارد، مانند سیسکو 7600 (یا سیسکو کاتالیست 6500) با یک VPNSM یا VPN SPA. بااین حال، یک کار وجود دارد که برخی از قابلیت‌های شتاب را در خود دارد (برای اطلاعات بیشتر به مقیاس طراحی، صفحه 41 نگاه کنید).

بیشترین استفاده معمول

طرح‌های توپولوژی spoke-to-spoke DMVPN معمولا تا زمانی که شرایط لازم برای مش پویا وجود داشته باشد استفاده می‌شود زیرا زمانیکه مشتریان پیش‌بینی می‌کنند که نیازهای ترافیکی قابل توجهی بین دفاتر شعبه وجود داشته باشد.

بااین‌حال، به‌دلیل محدودیت‌های فعلی QoS، اگر برنامه‌های کاربردی حساس به تاخیر / jitter / drop بر روی توپولوژی DMVPN مطرح گردند انتظارات باید به صورت مناسب تنظیم شوند. چنین طرح‌هایی در حال حاضر "بهترین تلاش" هستند.

برای کسب اطلاعات بیشتر در مورد استفاده از طرح‌های توپولوژی spoke-to-spoke DMVPN برای اتصال WAN، به راهنمای طراحی دینامیک VPNچندنقطه‌ای (DMVPN) در URL زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html.

طراحی مجازی تونل مجازی

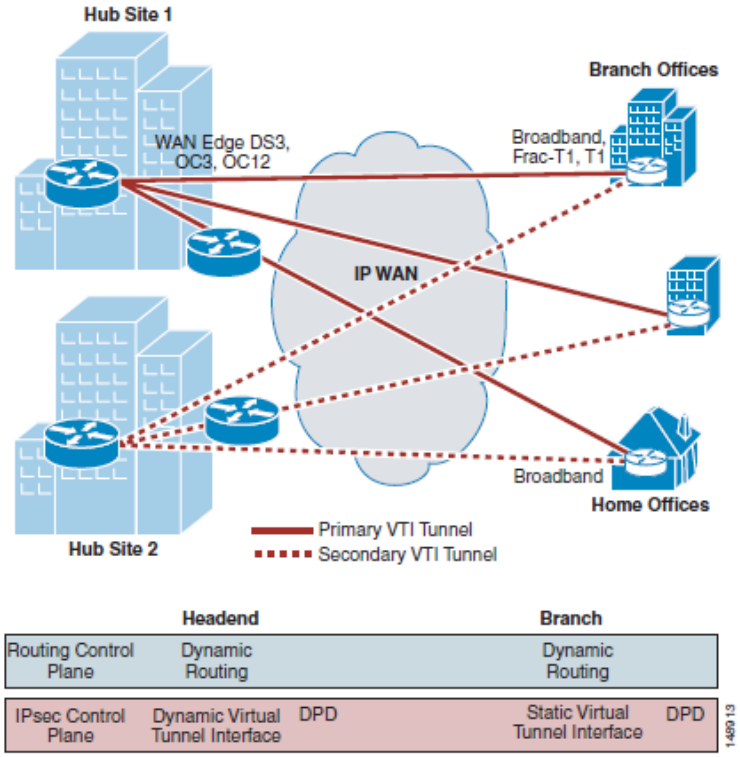
طراحی مجازی تونل مجازی (VTI) از جدیدترین گزینه‌های طراحی IPsec VPN موجود درIOS سیسکو است. طراحی VTI دارای تعدادی مزیت متمایز نسبت به سایر گزینه‌های طراحی IPsec است، از جمله توانایی انتقال پروتکل‌های مسیریابی پویا IGP و ترافیک IPmc بدون افزودن P2P GRE یا هدرهای mGRE.

علاوه براین، تونل‌های VTI دارای یک رابط هستند، به‌طوری‌که ویژگی‌های سطح تونل را می‌توان در هر تونل فعال کرد، به عنوان مثال یک سیاست سرویس QoS. این مسئله باعث می‌شود تا در یک تونل / مقصد VPN، QoS داشته باشیم.

بررسی اجمالی طراحی

شکل 15 طراحی VTI را نشان می‌دهد.

شکل 15 طراحی VTI



توپولوژی بسیار شبیه به P2P GRE در طراحی IPsec است، به جز زمانی که در ارتباط با سرویس مجازی استفاده می‌شود. همچنین VTI برخی مزایای مشابه‌ای با طراحی توپولوژیhub-and-spoke DMVPN ارائه می‌دهد.

هر سایت از راه دور با یک تونل VTI به یک headend از پیش تعریف شده متصل می‌شود. روترهای headend از رابط‌های پویا VTI برای پذیرش پویای اتصالات تونل جدید، بسیار شبیه رابط mGRE استفاده می‌کنند. به جز اینکه هر تونل جدید تعریف شده می‌تواند ویژگی‌های دیگری از یک تونل را مانند موارد دیگر به عنوان یک سیاست سرویس QoS ارائه دهد.

قابلیت تسریع با تطبیق تونل‌های VTI که در رابط‌های VTI در چند headend قرار دارند، در یک یا چند مکان جغرافیایی ارائه می‌شود.

ریموت‌ها می‌توانند IP های ایستا یا پویا داشته باشند، درحالی‌که headendsها باید آدرس‌های IP ثابت داشته باشند.

پروتکل مسیریابی پویا IGP بر روی تونل‌های VTI مبادله می‌شود و تونل‌های اولیه / ثانویه نیز با پیکربندی معیارهای مسیریابی کمی متفاوت هستند.

حفاظت از تونل IPsec به‌طورکلی برای نشان دادن ویژگی‌های رمزنگاری به تونلی که توسط آن ایجاد می‌شود استفاده می‌شود. DPD را می‌توان برای شناسایی از دست دادن اتصال peer فعال کرد.

مزایا

طرح‌های VTI مزایای زیر را ارائه می‌دهند:

• چندپخشی IP پشتیبانی می‌شود.

• پروتکل‌های مسیریابی پویا IGP بر روی تونل VPN پشتیبانی می‌شوند.

• پشتیبانی از اکثر سیستم‌عامل‌های روتر سیسکو IOS با T (14) 12.3 IOS یا 12.3 (4) شروع می‌شود.

• توزیع تونل IPsec به روتر headen ، با متریک‌های مسیریابی و همگرایی انتخاب بهترین مسیر قطعی است.

• تمام تونل‌های اولیه و ثانویه / پشتیبان گیری VTI از قبل ساخته شده‌اند، به‌طوری‌که یک تونل جدید نباید در صورت بروز یک سناریوی شکست ایجاد شود.

• پیکربندی VTI پویا است، که پیکربندی‌های headend را ساده و کوتاه می‌کند. فراهم کردن دفاتر شعبه جدید می‌تواند بدون تغییر پیکربندی / روترهای headend انجام شود.

• ممکن است در یک تونل VTI یک سرویس QoS اجرا کند (مقیاس‌پذیری می‌تواند جزء نگرانی‌ها باشد).

• هنگامی که خط مشی سرویس QoS برای VTI اعمال شود، IPsec anti-replay drop induced توسط رمزگذاری روترها به دلیل QoS انجام شده قبل از رمزگذاری حذف می‌شود. با این حال، توجه داشته باشید که ISP می‌تواند بسته‌ها را دوباره مرتب کرده و باعث ایجاد بسته ضدپاسخ شود.

• طراحی Encapsulation مستقیم IPsec در دیگر روترهای IOS سیسکو سازگار است زیرا یک مسیر مهاجرت از Headend طراحی Encapsulation مستقیم IPsec به VTI با هدایت پویا طراحی است.

معایب

طرح‌های VTI دارای معایب زیر هستند:

• IP Unnumbered مورد نیاز است.

• عدم پشتیبانی از پروتکل‌های غیر IP.

• ممکن است قابلیت همکاری محدود با دستگاه‌های مشابه غیرسیسکو داشته باشد.

• جفت‌های مسیریابی IGP تمایل دارند مقیاس‌پذیری طراحی را محدود کنند.

• سیاست‌های سرویس QoS در هر تونل به دلیل ترافیک عمومی موجود، محدودیت در مقیاس‌پذیری دارد.

• پشتیبانی از VTI در سیستم‌عامل‌های روتر بالا-پایان، مانند سیسکو 7600 (یا سیسکو کاتالیست 6500) با یک VPNSM یا VPN SPA وجود ندارد. VTI برای آینده Cisco IOS برنامه‌ریزی شده است.

بیشترین استفاده معمول

طراحی VTI نسبتا جدید است، اما می‌تواند برای همان نیاز مشتری نیز مورد استفاده قرار گیرد که در آن P2P GRE بر روی طراحی IPsec یا طرح توپولوژی DMUBP و DMVPN توصیه می‌شود؛ مثلا، جایی که الزامات حمل و نقل پروتکل‌های مسیریابی IGP و/ یا ترافیک چندپخشی IP بر روی VPN وجود دارد.

در مواردی که یک طراحی توپولوژی DMVPN hub-and-spoke در نظر گرفته می‌شود به دلیل پیکربندی ساده و تهیه بی نظیر شعبات جدید، طرح‌های VTI ساده‌تر از پیکربندی و طراحی بدون نیاز به پیکربندی mGRE یا NHRP ارائه می‌دهد.

علاوه براین، طراحی VTI قابلیت تنظیم پیکربندی سرویس QoS در سطح تونل را ارائه می‌دهد، که آن را تنها توپولوژی طراحی VPN می‌سازد که به راحتی می‌تواند QoS را در هر تونل / مقصد VPN پشتیبانی کند.

مقایسه‌ی طراحی‌ها

این بخش مقایسه‌ای از گزینه‌های مختلف طراحی شده در این راهنما را ارائه می‌دهد.

پشتیبانی از ویژگی های اصلی

جدول 3 برخی از ویژگی‌ها و الزامات اصلی را خلاصه می‌کند و نشان می‌دهد که آیا هر گزینه طراحی IPsec VPN از نیازمندی‌ها پشتیبانی می‌کند.

جدول 3. پشتیبانی از ویژگی‌های اصلی

	Dynamic Routing	Tunnel Keep-Alive	HA	IPmc	Interface QoS	Per-Tunnel QoS	Branch Dynamic IP Address	Dynamic Headend Config	Dynamic Meshing
IPsec Direct Encapsulation	Partial (DPD/RRI)	N/A	Stateful failover	No	Yes	No	Yes	Yes	No
p2p GRE Over IPsec	Yes	Yes	RP	Yes	Yes	Yes	Yes	p2p GRE, No IPsec, Yes	No
DMVPN Hub-and-Spoke Topology	Yes	No	RP	Yes	Yes	No	Yes	Yes	No
DMVPN Spoke-to-Spoke Topology	Yes	No	RP	Yes	Yes	No	Yes	Yes	Yes
VTI	Yes	No	RP	Yes	Yes	Yes	Yes	Yes	Yes

پشتیبانی از پلت‌فرم

جدول 4 پلت‌فرم کنونی روتر سیسکو IOS را خلاصه می‌کند و نشان می‌دهد که آیا هر یک از گزینه‌های طراحی IPsec VPN در پلتفرم امروزه پشتیبانی می‌شوند.

جدول 4. پشتیبانی از پلتفرم

	Cisco 870	Cisco ISR 1800	Cisco ISR 2800	Cisco ISR 3800	Cisco 7200VXR	Cisco 7301	Cisco 7600	Cisco Catalyst 6500
IPsec Direct Encapsulation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Point-to-Point GRE Over IPsec	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	Cisco 870	Cisco ISR 1800	Cisco ISR 2800	Cisco ISR 3800	Cisco 7200VXR	Cisco 7301	Cisco 7600	Cisco Catalyst 6500
DMVPN Hub-and-Spoke Topology	Yes	Yes	Yes	Yes	Yes	Yes	Work-around	Work-around
DMVPN Spoke-to-Spoke Topology	Yes	Yes	Yes	Yes	Yes	Yes	No	No
VTI	Yes	Yes	Yes	Yes	Yes	Yes	No	No

انتخاب طراحی

یکی از نقاط قوت سیسکو که باید به مشتریان ارائه شود، غنای گزینه‌های طراحی است که می‌تواند ارائه شود.

سوالات کلیدی زیر باید به مشتری کمک کنند که یک گزینه طراحی مناسب را انتخاب کند:

• فقط تک پخشی IP یا تک پخشی IP و چندپخشی IP ترکیب شده است؟

اگر ترافیک مشتری تنها IP Unicast باشد، و دفاتر شعبه نسبتا کوچک باشند، طراحی مستقیم Encapsulation IPsec ممکن است نیازهای شما را برآورده کند.

اغلب، مشتری‌ها، پروتکل‌های مسیریابی IGP یا IP چندپخشی در روش encapsulation مانند p2p GRE، mGRE، یا VTI نیاز دارند.

اگر مشتری نیاز به چندپخشی IP، پروتکل مسیریابی IG و پشتیبانی پروتکل غیر IP داشته باشد، تنها روش P2P GRE encapsulation پشتیبانی شده است.

• تعداد زیادی دفتر شعبه داریم یا کم؟

اگر استقرار مشتری برای تعداد نسبتا کمی از شعبات (100 یا بیشتر) باشد، طراحی P2P GRE بر روی IPsec ممکن است شرایط را برآورده کند.

اغلب مشتری به چندصد، هزار و چندین هزار شاخه دفتر مورد نیاز است، در این صورت پیکربندی headend پویا، مانند توپولوژی DMVPN یا طراحی VTI سودمند است.

• چه میزان از دسترسی مورد نیاز است؟

اگر نیاز مشتری برای 1-2 بار شکست خورده است، طراحی مستقیم IPsec ممکن است تنها گزینه طراحی باشد.

اگر مشتری انتظار 20-60 ثانیه شکست بر اساس همگام‌سازی مسیریابیIGP را داشته باشد، پروتکل‌های مسیریابی IGP با پشتیبانی از طرح، مانند p2p GRE برروی IPsec، توپولوژی DMVPN یا VTI باید درنظر گرفته شوند.

• اتصال پویا مورد نیاز است؟

اگر مشتری برای دفاتر شعبه خود و برای ایجاد ارتباط مستقیم با مشتری الزامات اساسی داشته باشد، به علت نیازهای مهم ترافیکی، طرحتوپولوژیDMVPN spoke-to-spoke به احتمال زیاد یکی از گزینه‌ها باشد.

مقیاس‌پذیری یکی دیگر از عواملی است که می‌تواند بر انتخاب طراحی تاثیر بگذارد، که در قسمت بعد پوشش داده می‌شود.

مقیاس‌پذیری یک طراحی

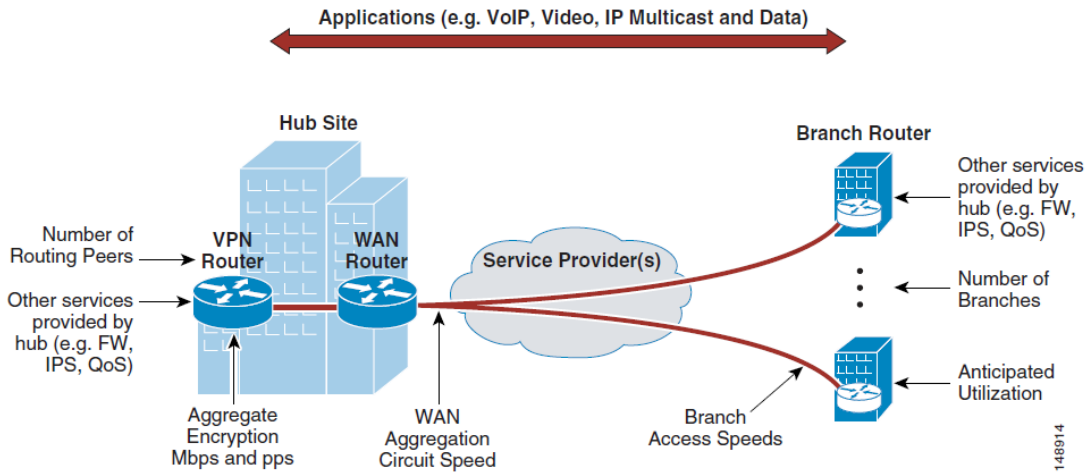
این بخش عوامل بحرانی را که بر مقیاس‌پذیری یک طراحی VPN IPsec تاثیر می‌گذارند، توضیح می‌دهد. در حالت ایده آل انتخاب طراحی و مقیاس‌پذیری طراحی باید تا حدودی از تصمیمات مستقل باشد، اما در حقیقت هر دو باید برای یک طراحی عملی مورد توجه قرار گیرند.

همچنین هر بخش طراحی را برای Encapsulation مستقیم IPsec، P2P GRE بر روی IPsec، DMVPN و VTI برای مقیاس‌پذیری و عملکرد خاص مشاهده کند.

معیارهای بحرانی مقیاس‌پذیری

مقیاس‌پذیری طراحی VPsp IPsec بستگی به تعدادی از عوامل دارد که بی‌اهمیت هستند. شکل 16 برخی از این عوامل را نشان می‌دهد.

شکل 16 معیارهای بحرانی مقیاس‌پذیری



عوامل اصلی در نظر گرفته شده شامل تعداد دفاتر شعبه، سرعت اتصال در هاب (ها) و شاخه‌ها (شعبات)، جفت‌های مسیریابی IGP، الزامات در دسترس بودن بالا و برنامه‌هایی که برر وی IPsec VPN منتقل می‌شوند، است. این عوامل بحرانی در بخش‌های زیر پوشش داده شده است.

تعداد دفاتر

تعداد دفاتر که بر روی VPN IPsec جمع می‌شوند عامل اصلی در تعیین مقیاس‌پذیری طراحی است.

علاوه بر اینکه یکی از عوامل اصلی طراحی است، تعداد دفاتر شعبه نیز بر روی برنامه‌ریزی مسیریابی، طراحی در دسترس بودن و در نهایت توان عمومی که باید توسط روتر headend (های) VPN جمع شوند تاثیر می‌گذارد.

تعداد دفاتر شعبه‌ای که امروز وجود دارد و همچنین نیازهای توسعه آینده را در نظر بگیرید.

سرعت اتصال

از آنجا که اتصالات VPN IPsec (معمولا) پهنای باند مرتبط با آنها را ندارند، به‌طورکلی رابط اتصال فیزیکی سرعت در هر دو روتر headend و شاخه به طور عمده حداکثر سرعت که VPN IPsec باید کار کند تعیین می‌کند. برخی از سرعت‌های اتصال معمولی در جدول 5 و جدول 6 نشان داده شده‌اند.

جدول 5. سرعت‌های اتصال headend

Connection Type	Speed
T3/DS3	44.76 Mbps
Fast Ethernet	100 Mbps
OC3	155 Mbps
OC12	622 Mbps

جدول 6. سرعت‌های اتصال شعبات

Connection Type	Speed
T1	1.544 Mbps
2 x T1	3.088 Mbps
T3/DS3	44.76 Mbps
Broadband cable/DSL	384 Kbps uplink / 2 Mbps downlink

بازده IPsec

بازده IPsec بستگی به عوامل متعددی دارد، از جمله سرعت اتصال، ظرفیت موتور رمزنگاری، و محدودیت روتر CPU.

بررسی انتقال دوجهته

اولین عامل مهم برای درک در مورد بازده IPsec،از طریق آن، یک موتور رمزنگاری IPsec در روتر IOS سیسکو است، که در آن نرم‌افزار و سخت‌افزار، یک دستگاه یک طرفه هستند که باید بسته های دو طرفه را پردازش کنند. بسته‌های خروجی باید توسط رمزنگاری IPsec رمزگذاری شوند، درحالی که ورودی بسته‌ها باید با همان دستگاه رمزگشایی

شود. بنابراین، برای هر رابط دارای بسته‌های رمزگذاری شده، لازم است که سرعت رابط دو طرفه را مورد توجه قرار دهیم. به عنوان مثال، سرعت اتصال T1 ، 1.544 مگابیت در ثانیه است، اما نیاز به IPsec 3.088 Mbps دارد.

تعداد بسته‌ها در هر ثانویه (pps) دقیق‌تر است

دومین عامل مهم برای فهم این مسئله این است که نرخ PPS مهمتر از کارآیی پهنای باند (bps) برای سرعت اتصال متوقف شده یا جمع شده است. به‌طورکلی روترها و موتورهای رمزنگاری مرزهای بالایی برای پردازش تعداد مشخصی از PPS ها دارند. اندازه بسته‌های مورد استفاده برای آزمایش و ارزیابی توانمندی‌ها می‌تواند عملکرد واقعی را کم و زیاد کند. به‌عنوان مثال، اگر روتر / ترکیب ماژولVPN بتواند 20 کیلو وات ساعت داشته باشد و سپس بسته‌های 100 بیتی به 16 مگابیت در ثانیه منجر شود بسته‌های 1400 بایت با همان سرعت بسته به 224 مگابیت بر ثانیه می‌رسند. به دلیل چنین واریانس وسیعی در بازده، PPS به طورکلی یک پارامتر بهتر برای بررسی مقیاس‌پذیری نسبت به bps است.

تعداد تونل‌ها می‌تواند یک عامل باشد

هر بار که یک موتور رمزنگاری یک بسته را رمزگشایی می‌کند، محاسبات ریاضی با استفاده از کلید رمزنگاری منحصر به فرد برای اعتماد، توسط فرستنده و گیرنده موافقت شده بر روی آن انجام می‌شود. اگر بیش از یک تونل IPsec در یک روتر خاتمه یابد، روتر دارای نقاط اعتماد و بنابراین چندین کلید رمزنگاری است. هنگامی که بسته‌ها ارسال می‌شوند یا به تونل دیگری از آخرین بسته فرستنده یا گیرنده ارسال می‌شوند، موتور رمزنگاری باید کلیدهای مبادله را برای استفاده از کلید درست همراه با نقطه اعتماد مورد استفاده قرار دهد. این تعویض کلید می‌تواند عملکرد موتور رمزنگاری را، بسته به معماری آن و افزایش مصرف روتر CPU کاهش دهد.

برای بعضی از سیستم‌عامل‌های سیسکو مانند VXR 7200 با SA-VAM2 +، همانگونه که تعداد تونل‌ها افزایش می‌یابد، ظرفیت موتور رمزنگاری IPsec کاهش می‌یابد. برای سایر سیستم عامل‌های سیسکو، مانند 7600 با VPN SPA، عملکرد نسبتا خطی و مشابه برای یک تونل به اندازه 1000 یا حتی 5000 است.

خلاصه عملکرد

عوامل متعددی وجود دارد (همانطور که در اینجا توضیح داده شد) که بر عملکرد تاثیر می‌گذارد، اما برای درک حداقل بازده کل IPsec که می‌تواند با سیستم‌عامل‌های مختلف به دست آید مفید است. جدول 7 فهرستی از ظرفیت هر پلت فرم را نشان می‌دهد.

جدول7. ظرفیت بازده IPsec توسط پلتفرم

Platform	Performance and Scalability Testing	Comparable Connection Speed
Cisco 1800 ISR On-board VPN Module	4–6 Mbps 2–2.5 Kpps	2 x T1
Cisco 2800 ISR On-board VPN Module	6–23 Mbps 2.5–11 Kpps	4 x T1
Cisco 3800 ISR On-board VPN Module	36–48 Mbps 18–24 Kpps	Fractional DS3
Cisco 7200VXR NPE-G1 Dual SA-VAM2+	80–100 Mbps 40–50 Kpps	DS3
Cisco 7600 Sup720 VPN SPA	1.1 Gbps–1.2 Gbps 480–600 Kpps	OC12

تست عملکرد و مقیاس‌پذیری نشان می‌دهد که چه چیزی تحت یک IP نسبتا Unicast با ترافیک تهاجمی (در ادامه شرح داده شده است) و پارامترهای عملکرد اندازه گیری شده است و می‌تواند توصیه طراحی در نظر گرفته شود. ستون سرعت اتصال قابل مقایسه، سرعت اتصال تقریبی را که می‌تواند توسط پلتفرم هدایت شود نشان می‌دهد.

جفت‌های مسیریابی

برای VPN های IPsec (مانند p2p GRE برروی IPsec، DMVPN و VTI)، تعداد جفت مسیریابی IGP که بایستی توسط روتر نگهداری شوند، عامل اصلی و تعیین کننده در مقیاس‌پذیری طراحی هستند.

عملکرد خاص بستگی به پلت‌فرم جمع‌کننده روتر و ظرفیت CPU آن دارد، که طراحی IPsec اجرا شده است، تعداد روترهای شعبات مبادله مسیریابی انجام داده‌اند و اینکه آیا تونلIPsec ثانویه (و پشتیبان) به سرآیند متناوب برای دسترسی بالا وجود دارد. جدول 8 محدوده‌های عمومی جفت‌های مسیریابی IGP را نشان می‌دهد که در آزمایشگاه سیسکو برای طرح‌های مختلف تایید شده است. جدول8. جفت‌های مسیریابی IGP توسط پلتفرم

Platform	Performance and Scalability Testing
Cisco 7200VXR NPE-G1 Dual SA-VAM2+	500–700
Cisco 7600 Sup720 VPN SPA	1000

نکته: این که آیا یک پلت‌فرم و طراحی واقعا می‌تواند تعدادی از همتایان پیشنهاد شده در اینجا را که بستگی به همه عوامل دیگر دارد و در این قسمت پوشش داده شده است به کار می‌برد.

کیفیت خدمات

تأثیر QoS در مقیاس‌پذیری به‌طور عمده بستگی به دامنه‌ای که QoS در آن مستقر است دارد. اگر در سطح رابط مستقر شود، مقیاس‌پذیری و اثرات تست عملکرد در روتر سیسکو IOS زمانی که QoS و به طور خاص شکل‌گیری ترافیک (GTS) درگیر هستند تقریبا 10 تا 15 درصد نشان داده است. این مسئله در درجه اول قرار دارد زیرا GTS تغییر فرایند است، نه تغییر CEF.

اگر یک الزام برای QoS تونل برای هر VPN وجود داشته باشد، این به این معنی است که تعدادی از اپراتورهای ترافیک به طور همزمان در روتر سیسکو IOS در طول دوره تجمع تونل درگیر هستند. به دلیل فرایند تعویض، اگر شمار قابل توجهی از تصحیح‌کننده‌های ترافیک در یک پلت‌فرم درگیر شوند، مقیاس‌پذیری به شدت محدود می‌گردد.

در دسترس بودن بالا

ماهیت الزامات طراحی در دسترس بودن بالا بر استقرار مقیاس‌پذیری تاثیر می‌گذارد. اگر چندین headend در یک سایت جغرافیایی مختلف با هر روتر دارای یک تونل IPsec با headends اولیه یا ثانویه (و احتمالا پشتیبان) مستقر شوند، تعداد کل تونل‌های IPsec که باید جمع شوند دو برابر می‌شود (یا سه برابر و یا حتی چهار برابر).

به عنوان مثال، اگر 300 شعبه در یک جفت روتر headend جمع گردند، و هر کدام یک تونل اولیه و ثانویه داشته باشند، در مجموع 600 تونل وجود دارد. اگر یک مرکز داده پشتیبان دوم با دومین جفت از روترهای headend گنجانده شود، بالغ بر 1200 تونل کامل از این 300 شاخه وجود دارد.

زمان همگام بودن در دسترس بودن بالا، پس از شکست نیز یک عامل مهم در مقیاس‌پذیری طراحی است. به عنوان مثال، اگر یک VPN روت شده IPsec VPN نیاز به همگرایی در ظرف 20 ثانیه داشته باشد، فرکانس مسیریابی hellos باید از یک طراحی با الزام همگرایی 40 ثانیه بیشتر باشد. زمان همگرایی تهاجمی، موجب بار بیشتر در headend روتر CPU برای پردازش تعداد hellos فرستاده شده یا دریافت شده به همه جفت‌ها (شعبات دفتر) می‌گردد.

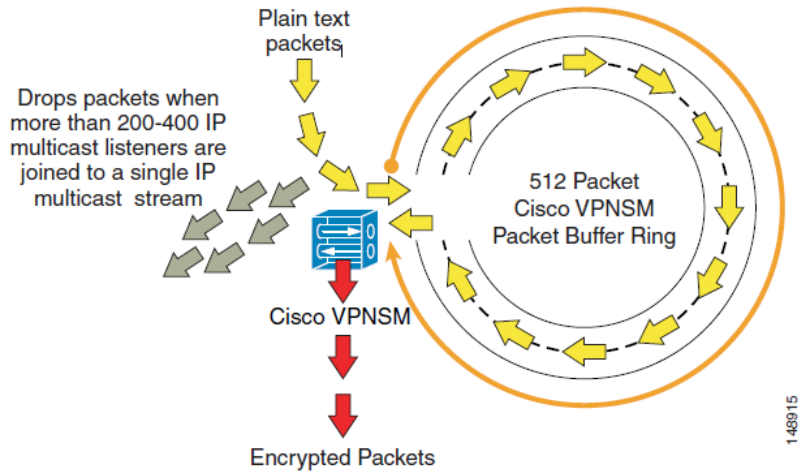
چندپخشی IP

اگر چندپخشی IP جزء نیازمندی‌های طراحی باشد، قطعا می‌تواند مقیاس‌پذیری یک طراحی VPsp IPsec را محدود کند. همان‌طورکه قبلا ذکر شد، طراحی P2P GRE بر روی IPsec، DMVPN، یا VTI باید برای انتقال IP در ترافیک چندگانه انجام شود.

چندپخشیIP به روترheadend رمزگذاری برای تکثیر هر بسته چندپخشی IP برای هر تونل VPN نیاز دارد که به جریان چندپخشی IP متصل است. سرعت خروجی IP multicast باعث ایجاد چالش‌هایی برای پشتیبانی از تعداد قابل توجهی از شنوندگان چندپخشی IP متصل به یک جریان چندپخشی IP منحصربفرد بدون پیوستگی در صف ورودی موتور رمزنگاری در یک پلتفرم داده شده می‌شود.

برای مثال، تست مقیاس‌پذیری و عملکرد با VPNSM سیسکو (در هر دو 6500Catalyst Cisco و سیسکو 7600) نشان داده است که هر بار که تعداد IP های شنونده چندرسانه‌ای به یک جریان چندپخشی IP متصل می‌شوند بیش از 200 تا هستند. شکل 17 این موضوع را نشان می‌دهد.

شکل 17 مسائل حلقه بافر چندپخشی IP



جدیدترین SPA VPN سیسکو با توانایی مدیریت تا 1000 شنونده متصل به یک جریان چندپخشی تک را به طور همزمان بهبود داده است.

برای کسب اطلاعات بیشتر در مورد پشتیبانی از برنامه‌های چندرسانه‌ای IP بر روی IPsec VPN، به راهنمای طراحی Multicast IP بر روی IPsec VPN در URL زیر مراجعه کنید:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc..html

استراتژی دسترسی به اینترنت

چگونگی انتقال ترافیک اینترنت از دفاتر شعبه نیز می‌تواند بر طراحی VPN IPsec مقیاس‌پذیری تاثیر بگذارد. که در درجه اول زمانی که اینترنت به عنوان انتقال اتصال به شعبات استفاده می‌شد در نظر گرفته شده است. دو گزینه مشترک در دو بخش بعدی با مفاهیم مقیاس‌پذیری طراحی شرح داده شده است.

backhaul

مشتریان شرکت معمولا انتخاب می‌کنند که تمام ترافیک را به سایت headend بازگردانند، صرف نظر از اینکه آیا ترافیک برای شبکه شرکتی یا برای اینترنت تعیین شده است. ممکن است برای رمزگذاری و انتقال ترافیک اینترنت بر روی اینترنت از طریق یک تونل IPsec، فقط برای رمزگشایی به نظر ناکارآمد باشد. اما احتمالا از همان دروازه که بسته بود وارد شوند.

با این وجود، دلایل قانونی برای انجام این کار وجود دارد، از جمله:

• حفظ مسیریابی شعبه به دلایل امنیتی ساده، به جای پیکربندی پیچیده‌تر برای ارسال ترافیک بر روی تونل شرکت و دیگر ترافیک مستقیم به اینترنت.

• نظارت بر ترافیک اینترنت مانند فیلتر URL، Websense، اسکن ایمیل و اسکن ضد ویروس، می‌تواند در محل (ها) دفتر مرکزی شرکت برای مدیریت در توابع نظارت توزیع شده متمرکز گردد.

اگر تمام ترافیک، از جمله مقصد اینترنت، بر روی اتصال VPN IPsec پشتیبانی شود، این ترافیک باید به پهنای باند ترافیکی عمومی و نیازهای بازده IPsec برای طراحی توجه کند.

تونل زنی تقسیم شده

تونل‌زنی تقسیم شده فرایندی است که بسته‌ها را از یک شعبه منتقل می‌کند و می‌تواند توسط IPsec و فرستادن یا دریافت از روتر تجمع headend محافظت شده باشد، یا توسط IPsec و ارسال یا دریافت از اینترنت محافظت نشده باشد.

اگر تونل‌زنی تقسیم شده اجرا شود، در طراحی باید عوامل اضافی زیر را در نظر گرفت:

پهنای باند و توان IPsec با مسیریابی ترافیک اینترنت به جای VPN به دفتر مرکزی

به احتمال زیاد NAT یا PAT باید به عنوان یک سرویس در روتر اداره شوند، که می‌تواند پیامدهای عملکرد و مقیاس‌پذیری داشته باشد.

خدمات امنیتی مانند فایروال و IPS ممکن است به‌عنوان خدمات در روتر شعبه اداره شوند، که دارای پیامدهای عملکردی و مقیاس‌پذیری هستند. آیا سرویس‌های امنیتی که در روتر شاخه در حال اجرا هستند یا به‌عنوان دستگاه های جداگانه در نظر گرفته می‌شوند اجباری هستند یا خیر.

آیا ترافیک اینترنت به دلیل تقسیم شدن از ترافیک محافظت شده IPsec است؟ در کدام زیرشبکه (ها) یا VLAN (ها) میزبان در شاخه واقع شده است؟

سرویس‌های یکپارچه

سرویس‌های یکپارچه که در حال اجرا بر روی روترهای یکسانی به عنوان VPN IPsec هستند باید در کل مقیاس‌پذیری مورد توجه قرار گیرند، زیرا بسته به سیستم عامل، سرویس‌های اضافی می‌توانند عملکرد روتر را تحت تاثیر قرار دهند. نمونه‌هایی از خدمات یکپارچه در بخش‌های بعدی پوشش داده می‌شود.

امنیت

سرویس‌های یکپارچه امنیتی می‌توانند شامل فایروال، IPS، پیشگیری از DoS، کنترل دسترسی شبکه (NAC) وغیره باشند. خدمات امنیتی معمولا در حین انجام بازرسی و تجزیه و تحلیل بسته به شدت محاسباتی هستند.

سرویس‌های یکپارچه امنیتی ممکن است بسته به نوع عملکرد و سطح شتاب در سخت افزار که در پلت فرم خاص ارائه شده است، بر عملکرد روتر تاثیر مستقیمی داشته باشند. اگر سرویس‌های امنیتی در پردازنده اصلی روتر انجام شوند، این سرویس به احتمال زیاد بر عملکرد تاثیر می‌گذارد.

سرویس‌های یکپارچه امنیتی بیشتر در روترهای شعب اداره شوند، اما به‌طور فزاینده‌ای در روترهای تجمع سرآیند نیز، به ویژه در شرایطی که یک سرویس حمل و نقل غیرقابل اعتماد، مانند اینترنت وجود دارد، برای حمل و نقل WAN یا VPN استفاده می‌شوند.

VoIP

خدمات صوتی یکپارچه شامل کارت‌های ایستگاه صوتی هستند که handsetها، کنفرانس VoIP و خدمات انتقال از قبیل پردازنده‌های سیگنال دیجیتال (DSPs)، شبکه تلفن عمومی (PSTN)، تلفن همراه (SRST) و سایر موارد را خاتمه می‌دهند.

خدمات صوتی یکپارچه در روترهای دفتر شعبه، به ویژه با خدمات یکپارچه(ISR) رایج هستند، که به طور خاص با خدمات یکپارچه در ذهن طراحی شده‌اند. خدمات صدای یکپارچه به‌طورکلی در روترهای تجمعی headend مستقر نمی‌شوند.

سایر خدمات یکپارچه

انواع دیگر خدمات یکپارچه که می‌توانند عملکرد روتر را تحت تاثیر قرار دهند عبارتند از:

- NAT یا PAT
- سرور DHCP
- ذخیره محتوا

برای اطلاعات بیشتر در مورد تاثیرات ویژه این خدمات راهنماهای طراحی IPsec Individual برای Encapsulation مستقیم IPsec، P2P GRE بر روی IPsec، DMVPN، و VTI را ببینید.

پیوست A–ارزیابی مقیاس‌پذیری طراحی

این پیوست توضیح می‌دهد که چگونه سیسکو آزمایش عملکرد و مقیاس‌پذیری را انجام می‌دهد.

روش آزمایش

روش تست سیسکو این است که شبکه‌هایی را با استفاده از بهترین شیوه‌ها ایجاد می‌کند و سپس بارهای ترافیکی که تقریبا نزدیک به شبکه‌های واقعی مشتری هستند اعمال می‌کند. چند تست اثبات مفهوم وجود دارد که به خوبی تست بزرگی در مقیاس نزدیک به 1500 روتر عمل می‌کنند، که قادر (با استفاده از VRFs) به تقلید کردن تا 5000 روتر شاخه با توانایی ترافیک مشتری 1.5 گیگابیت در ثانیه هستند.

اهداف آزمون عبارتند از یافتن عملکرد دنیای واقعی و مقیاس‌پذیری برای سیستم عامل سیسکو در یک سیستم پایان به پایان است. هدف این نیست که به‌طورکامل تمام ویژگی‌ها و عملکرد و همچنین حداکثر امتیاز عملکرد سیستم عامل تست شوند. در عوض هدف این است که توصیه‌ها را برای استفاده در اندازه‌گیری طرح های مشتری ارزیابی کنیم.

ترافیک ترکیبی

سیسکو سوالهای زیادی را در مورد مشتریان در رابطه با آزمایش با اندازه‌های خاص بسته و یا با تست محبوب IMIX جواب داده است. سیسکو با اندازه بسته‌ی خاصی آزمایش نمی‌کند و از IMIX استفاده نمی‌کند. همانطور که قبلا ذکر شد، روش تست برای اعمال پروفایل‌های واقعی ترافیک مشتری، به عنوان نقاط انتهایی سرور است (مانند Sun Netras یا Penguins) که برای ایجاد جریانهای پروتکل انتها به انتهای شبکه استفاده می‌شوند.

جریانهای ترافیکی در درجه اول با استفاده از ابزار تست Chariot NetIQ و Ixia ایجاد می‌شوند. ترکیبی از ترافیک در درجه اول از انواع ترافیک تشکیل شده است:

- DNS
- FTP
- POP3
- HTTP
- TN3270
- g.729 VoIP

ترکیبی از ترافیک تقریبا 35 درصد UDP و 65 درصد TCP در bps است که با ~ 80 درصد از بسته‌های UDP، با 20 درصد باقیمانده TCP همبستگی دارد. در بسته‌های UDP، اکثریت جریان‌های g.729 VoIP RTP برای شبیه‌سازی یک شبکه سازمانی همگرا است. دستورالعمل‌های اکشتافیVoIP و QoS بیان می‌کنند که پهنای باند مصرفی VoIP نباید بیش از 33 درصد پهنای باند کل bps باشد.

تاثیر قابل توجه این مشخصات ترافیک، در مقایسه با یک پروفایل مانند IMIX، این نتایج را به همراه8 دارد که برای یک شبکه داده تنها مناسب است. IMIX، VoIP را به عنوان ورودی VoIP قبول نمی‌کند. ورود VoIP موجب افزایش تعداد بسته‌های کوچک در ترافیک ترکیب شده و نرخ کلی PPS می‌گردد.

یافتن محدودیت‌ها

یافتن محدودیت‌های عملکرد یک فرایند دشوار است، زیرا برای تعیین میزان BPS یا PPS خاص بسیار دشوار است. اساسا آنچه اتفاق می‌افتد، یک فرایند تکراری است که جریان‌های ترافیکی را افزایش می‌دهد درحالی‌که نسبت پروتکل‌ها، تا زمانی که محدودیت‌های مورد نظر یافت نشوند تعریف شده است.

جدول9. یافتن محدودیت‌ها

Parameter	Acceptable Value
CPU	Performance reported at 50%, 65%, and 80% points
Latency	<50ms one way
Jitter	<10ms one way
Packet drops	<0.5%
Process switching	Monitored
Anti-replay drops	<1%
Failover	Must converge and continue operation in a reasonable time frame

استفاده از CPU هدفمند برای راه اندازی روتر همیشه مورد بحث است. سیسکو تلاش می‌کند یک دامنه نمایشی از بهره برداری از CPU بالاتر از استقرار شبکه معمولی ارائه دهد. این بهره‌برداری‌ها 50 درصد، 65 درصد و 80 درصد

است. گرچه تعداد زیادی (80 درصد) در عملیات عادی توصیه نمی‌شوند، این عدد برای فعال کردن یک مهندسی شبکه برای مشاهده سطوح ترافیک می‌تواند توسط یک پلت فرم در یک سناریو شکست خورده انجام شود.

نتایج

نتایج سیسکو و مقیاس‌پذیری به نظر می‌رسد محافظه کارانه باشند. این نتایج به معنای مخالفت آنها با داده‌های عملکرد داده شده در جدول داده‌ها برای محصولات نیست. در عوض آنها رهنمودهای عملکرد طراحی محافظه کارانه را که می‌تواند برای استقرار با سطح اطمینان استفاده شود در نظر گرفته‌اند.

هر آزمایش دارای مجموعه‌ای از محدودیت‌های خاص خود است. به یاد داشته باشید که نتایج آزمون سیسکو نتایج خاصی برای یک مجموعه خاص از شرایط و شرایطی را که می‌تواند در هر شبکه مشتری رخ دهد، منعکس نمی‌کند.

بسترهای ارزیابی شده سیسکو

جدول 10 سیستم‌های مختلفی را نشان می‌دهد که در آزمایشگاه IPsec VPN Cisco مورد ارزیابی قرار گرفتند.

جدول 10. بسترهای ارزیابی شده سیسکو

Application	Cisco VPN Router	Processing Engine	VPN Acceleration Options
Headend aggregation	Catalyst 6500	Sup2	VPNSM
	7600	Sup 720	VPN SPA
	7200VXR	NPE-G1	SA-VAM2+
	7301	NPE-G1 (Equivalent)	SA-VAM2+
Large branch office	3845 ISR	On-Board	On-Board, AIM-VPN/HP/II+ (optional)
	3825 ISR	On-Board	On-Board, AIM-VPN/EP/II+ (optional)
Medium branch office	2851 ISR	On-Board	On-Board, AIM-VPN/EP/II+ (optional)
	2821 ISR	On-Board	On-Board, AIM-VPN/EP/II+ (optional)
	2811 ISR	On-Board	On-Board, AIM-VPN/EP/II+ (optional)
Small office	2801 ISR	On-Board	On-Board, AIM-VPN/EP/II+ (optional)
	1841 ISR	On-Board	On-Board, AIM-VPN/BP/II+ (optional)
	1811W	On-Board	On-Board
	871W	On-Board	On-Board

شکل 11. بسترهای ارزیابی شده VPNسیسکو

Application	Cisco VPN Router	Processing Engine	VPN Acceleration Options
Headend aggregation	7200VXR	NPE-400	SA-VAM
	7200VXR	NPE-300	SA-VAM
Large branch office	3745	On-Board	AIM-VPN/HPII
	3725	On-Board	AIM-VPN/EPII
Medium branch office	2691	On-Board	AIM-VPN/EPII
	2651XM	On-Board	AIM-VPN/BPII
	1760	On-Board	MOD1700-VPN
Small office	1711	On-Board	On-Board
	831	On-Board	On-Board

پیوست B- منابع توصیه شده برای مطالعه

این بخش مراجع زیر و اطلاعات اضافی مرتبط با موضوعات تحت پوشش در این راهنمای طراحی را فراهم می‌کند:

• اسناد:

- IPsec Direct Encapsulation Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html

- Point-to-Point GRE بر روی IPsec Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2 P_GRE_IPSec.html

- راهنمای طراحی VPNپویا چند نقطه (DMVPN)

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html

-راهنمای طراحی Voice and Video Enabled IPsec VPN (V3PN)

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRSRND.html_ND/V3PN

- راهنمای طراحی چندرسانه ای بر روی IPsec VPN

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html

- V3PN: طراحی مجدد بارگذاری و تعادل بار

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/VPNLoad/VPN_Loa d.html

- گواهینامه های دیجیتال / PKI برای IPsec VPNs

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/DCertPKI.html

- پروژه QoS SRND

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-S RND-Book.html

• درخواست مقاله (RFC)

- معماری امنیت برای پروتکل اینترنت - RFC 2401

- سرآیند اعتبارسنجی IP - RFC 2402

- استفاده از HMAC-MD5-96 در ESP و AH-RFC 2403

- استفاده از HMAC-SHA-1-96 در ESP و AH-RFC 2404

- الگوریتم رمزنگاری ESP DES-CBC با IV-RFC 2405

- امنیت IP Encapsulating Payload (ESP)-RFC 2406

- دامنه امنیت اینترنت IP برای ISAKMP-RFC 2407

- پروتکل مدیریت اینترنت و کلید RFC 2408- (ISAKMP)

- کلید تبادل اینترنتی RFC 2409- (IKE)

- الگوریتم رمزگذاری NULL و استفاده از IPsec-RFC 2410

- سند IP Security Document Roadmap- RFC 2411

- پروتکل تعریف کلید OAKLEY-RFC 2412

پیوست C-مخففها

واژه	تعریف
3DES	استاندارد سه بعدی رمزگذاری اطلاعات
AES	استاندارد رمزگذاری پیشرفته
AIM	ماژول ادغام پیشرفته
ATM	حالت انتقال آسنکرون
CA	گواهینامه صف بندی
CBWFQ	صفبندی صفر براساس کلاس
CPE	طبقهبندی تجهیزات مشتری
DES	استاندارد رمزگذاری داده
DHCP	پروتکل پیکربندی پویا میزبان
DMVPN	شبکه خصوصی مجازی چند نقطهای
DPD	Dead Peer Detection
DSL	خط مشترک دیجیتال
EIGRP	پروتکل مسیریابی پیشرفته
FRTS	شکل دادن به ترافیک
FTP	پروتکل انتقال فایل
GRE	مسیریابی عمومی
HSRP	پروتکل مسیریابی داغ
IKE	تبادل کلید اینترنت
IOS	سیستم عامل اینترنت
IPmc	چندپخشی IP
IPsec	امنیت IP
ISP	ارائهدهنده خدمات اینترنتی
LFI	تقسیم بندی Link و Interleaving
mGRE	Multipoint Generic Route Encapsulation
MPLS	سوئیچینگ برچسب چند پروتکلی
NAT	ترجمه آدرس
NHRP	پروتکل hub بعدی
OSPF	باز کردن کوتاهترین مسیر
P2P GRE	GRE نقطه به نقطه

PAT	ترجمه آدرس پورت
PVC	پورت مدار مجازی
QoS	کیفیت خدمات
RADIUS	اعتبارسنجی از راه دور در سیستم کاربر
RTP	روتکل زمان واقعی
SLA	توافق نامه سطح سرویس
SPA	آداپتور پورت مشترک
SRST	پورتال قابل استفاده از راه دور
TCP	پروتکل کنترل انتقال
ToS	نوع خدمات
UDP	پروتکل دیتاگرام کاربر
VoIP	Voice over IP
V3PN	Voice و Video Enabled IPsec VPN
VAM	VPN Acceleration Module
VPN	شبکه خصوصی مجازی
VPNSM	ماژول سرویس VPN
VPN SPA	آداپتور اشتراک پورتVPN
VTI	رابط تونل مجازی
WAN	شبکه گسترده