بسم الله الرحمن الرحيم

شكر وتقدير

أولاً الشكر لله عز وجل، ثم لوالدينا على جهودهم التي بذلوها في مساعدتنا على الوصول الى ما وصلنا اليه.

يسرنا أن نوجه الشكر لكل من نصحنا أو أرشدنا أو وجهنا أو ساهم معنا في إعداد هذا البحث بإعلامنا عن المراجع والمصادر المطلوبة في مراحله المختلفة، ونشكر على وجه الخصوص استاذنا الفاضل المهندس (ماجد خلف البدراني) على مساندتنا وإرشادنا بالنصح والتصحيح .

الفهرس

- **إسم المشروع**

ربط فرع الجامعة بالمبنى الرئيسى للجامعة باستخدام تقنية الشبكة الخاصة الافتراضية (VPN) مع شبكة ال DMZ وخدمات شبكية أخرى

- **المقدمة**
  - فى هذا المشروع يتم عمل شبكة موسعة تتكون من شبكة محلية بالمبنى الرئيسى للجامعة بها تقنيات مختلفة سيتم ذكرها فيما بعد تضمن جودة الأداء والعمل ونقل البيانات بانسيابية بين موارد الشبكة من أجهزة حاسب آلى وخوادم وطابعات و أجهزة الإتصال الصوتى وخدمة الإنترنت ، كما سيتم ربط المبنى الرئيسي للجامعة بالمبنى الفرعي لها وذلك عن طريق تقنية الشبكة الخاصة الافتراضية (VPN) من خلال الإنترنت لكى توفر إستخدام موارد الشبكة المحلية بالمبنى الرئيسي لمستخدمي ومنسوبى فرع الجامعة، وكذلك تصميم شبكة وسطية بها خوادم وتطبيقات تكون متاحة للإستخدام من خلال الإنترنت

- **معلومات عامة عن الشبكات**
  - شبكة الحاسوب هي مجموعة من اجهزة الحاسوب متصلة مع بعضها بوسائل الربط المختلف لتسهيل عملية الاتصال فيما بينها ومشاركة الملفات والبيانات والمعلومات وحتى الاجهزة مثل الطابعات وغيرها، وتساعد الشبكات وبشكل كبير على تسهيل القيام بالأعمال وإنجازها

  - **انواع شبكات الكمبيوتر حسب طريقة التوصيل**
    - الشبكة الخطية : وهي الشبكة التي ترتبط فيها جميع الأجهزة من خلال خط واحد من الأسلاك، وتعد الشبكة الخطية من

أرخص أنواع الشبكات ومن أسهلها من حيث إضافة أي جهاز الى الشبكة، وتتعطل هذه الشبكة بشكل تام إذا حدث أي قطع في الكيبل المركزي للاجهزة.

- شبكة النجمة: وهي الشبكة التي تتوزع فيها أجهزة الكمبيوتر حول جهاز مركزي، ويتم فيها توصيل البيانات من جهاز الى جهاز اخر عن طريق الشبكة مروراً بالجهاز المركزي، ومن مميزات هذه الشبكة عدم تأثرها بتعطل أي جهاز كمبيوتر فيها، ولكن إذا تعطل الجهاز المركزي فإن الشبكةبأكملها سوف تتعطل.
- الشبكة الحلقية: وهي التي تتصل فيها أجهزة الكمبيوتر على شكل حلقة مغلقة، فعندما نرسل رسالة في هذه الشبكة فإنها تمر الى جميع الأجهزةالموجودة بين المرسل والمستقبل.

- **انواع الشبكات حسب حجمها**

- الشبكة المحلية: وهي شبكة عبارة عن مجموعة من أجهزة الحاسوب التي تتصل مع بعضها لبعض في مساحة جغرافية صغيرة، وتنتمي أجهزة الكمبيوتر في الشبكة المحلية إلى نفس المؤسسة، وتعتبر الشبكة المحلية من أبسط أشكال شبكات الكمبيوتر، كما تصل سرعة نقل البيانات في هذه الشبكة إلى 1 ميجابت في الثانية، ويمكن أن تصل إلى 10 جيجابت في الثانية.
- الشبكة الاقليمية: وهي الشبكة التي تربط بين عدة شبكات محلية ضمن مساحات جغرافية متوسطة في الحجم قد تصل إلى عدة أميال، وفي العادة يتم ربط الشبكة الإقليمية عن طريق وسائط اتصال عالية السرعة مثل كيبلات الألياف الضوئية.
- الشبكة الواسعة: وهي تلك الشبكات التي تغطي مساحات جغرافية كبيرة جدا، وتعد شبكة الإنترنت العالمية هي من أحد أشهر الأمثلة على الشبكات الواسعة، وهي تختلف سرعة الشبكات الواسعة حسب اختلاف وسائل الاتصال المستخدمة.

- **مخاطر أمن شبكات المعلومات**

يمكننا تصنيف الجرائم التي تتم عن طريق استخدام تكنولوجيا المعلومات إلى عدة أقسام وكل قسم يختص بنوع معين من الجرائم التي يمكن ارتكابها وهي كالتالي:

- جرائم تهدف لنشر معلومات

في مثل هذا النوع يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات على الملأ، ومن أمثلة ذلك نشر معلومات بطاقات الائتمان البنكية، وأرقام الحسابات المصرفية، وأيضاً نشر المعلومات الاستخباراتية المتعلقة بدول أو أشخاص

- جرائم تهدف لترويج الإشاعات

وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات .

- جرائم التزوير الإلكترونية

وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، مثل تزوير البطاقات الائتمانية وجوازات السفر وغيرها من الأوراق الرسمية والثبوتية ، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.

- جرائم تقنية المعلومات

وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية، مثل برامج التشغيل أو البرامج التطبيقية غالية الثمن، والتي يتم تقليدها عن طريق قراصنة.

- نطاق المشروع

مبنى الجامعة الرئيسى ومبنى فرعى تابع للجامعة

- الخدمات المقدمة

تركيب و إعداد جهاز فيروول بالمبنى الرئيسي و آخر بالمبنى الفرعي وربطهم معاً باستخدام تقنية الشبكة الخاصة الافتراضية (VPN)، مع توفير شبكة وسطية (DMZ)بها الخوادم المطلوب الوصول إليها من قبل مستخدمي الإنترنت وكذلك مستخدمي الشبكة الداخلية، كما سيتم تركيب واعداد سويتش رئيسي core switchو آخر بديل backup switchفي الشبكة الرئيسية للجامعة واستخدام تقنية HSRPوتفعيل خاصية Ether Channelبينهما، وتوزيع حركة مرور الحزم عليهما باستخدام VLANs و SVIsو تفعيل ال NAT للوصول الى الانترنت

وأخيراً تفعيل خدمة QOS التى تعمل أولوية للرسائل الصوتية والفيديو على الرسائل النصية

- الأنظمة
  - CISCO core and backup, access switches, ASA,Servers, Firewall, DMZ

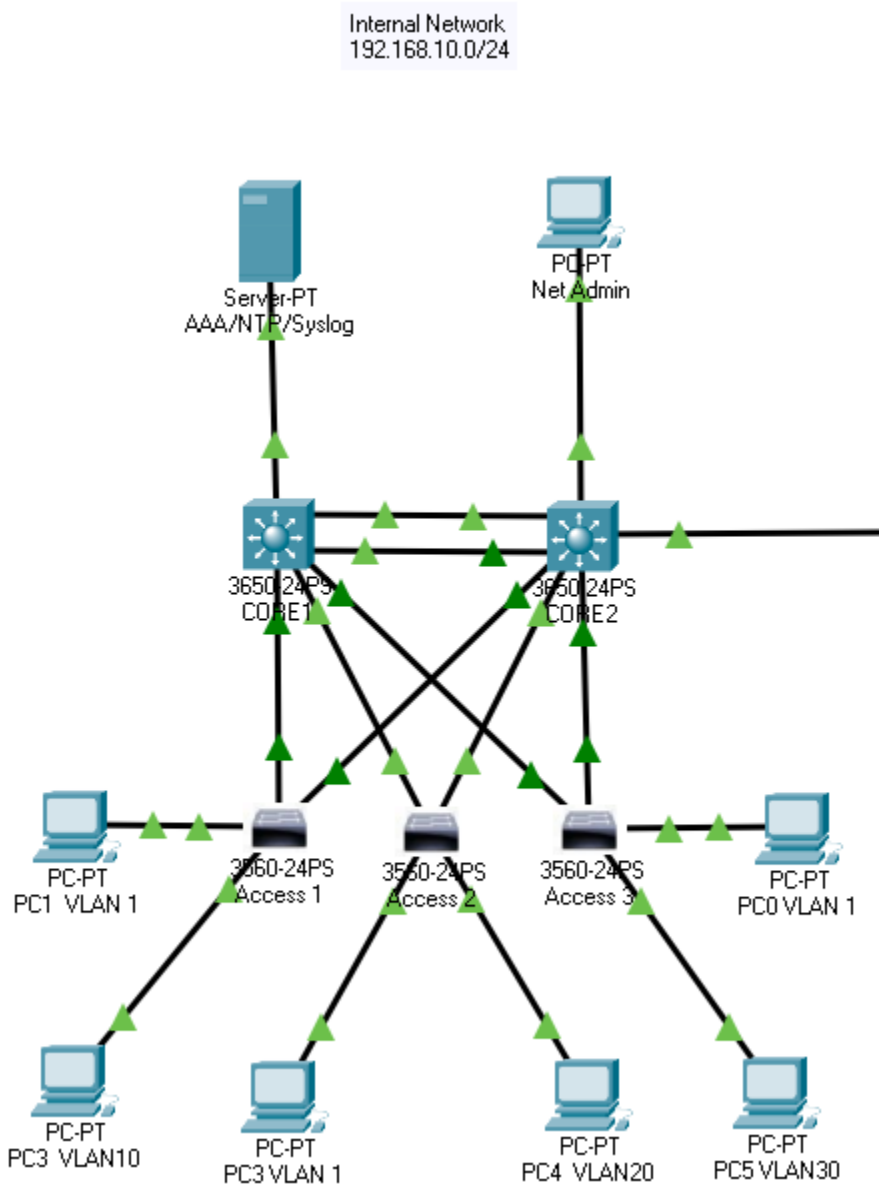
- التقنيات المستخدمة
  - VPN, IPS, Packet filtering, Internet, NAT, VTP, HSRP, Trucking, DNS, SVI, DHCP

- الأهداف
  - إنشاء خوادم عامة بمنطقة (DMZ)
  - إنشاء جدار حماية محيط
  - تبني نهج متعدد الامان
  - رابط الفروع بتقنية VPN
  - شبكة ذات توافر عالي (High Availability)
  - شبكة توازي للحمل (Load Balancing)
  - توفر جودة الخدمة (Quality of service)
  - الاتصال عن بعد VPN

طوبولوجيا الشبكة

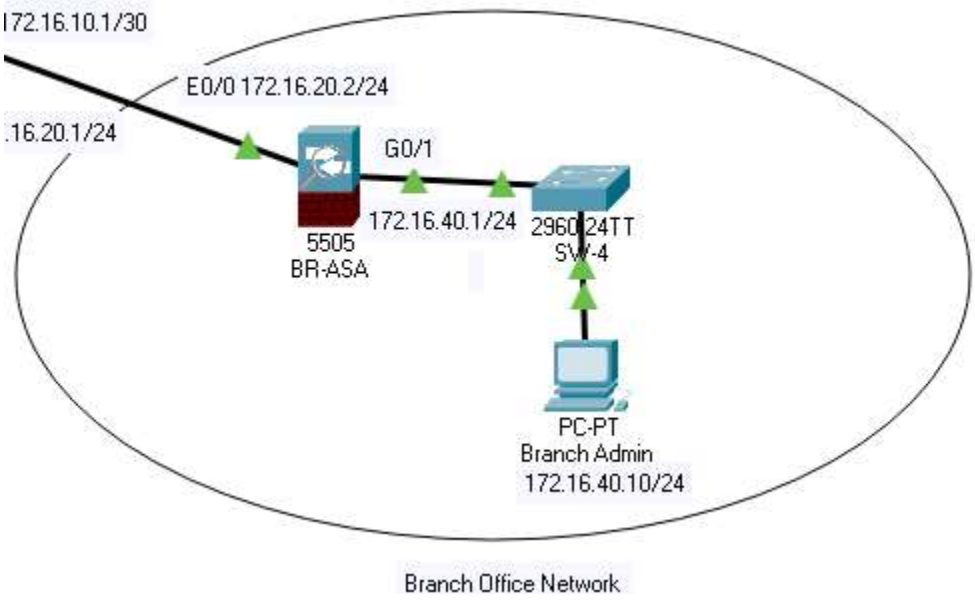
تتكون الشبكة من الآتى :

١- شبكة داخلية بالمبنى الرئيسي للجامعة بها طبقتين مختلفتين من حيث دورها فى توزيع مرور المعلومات بمختلف أنواعها



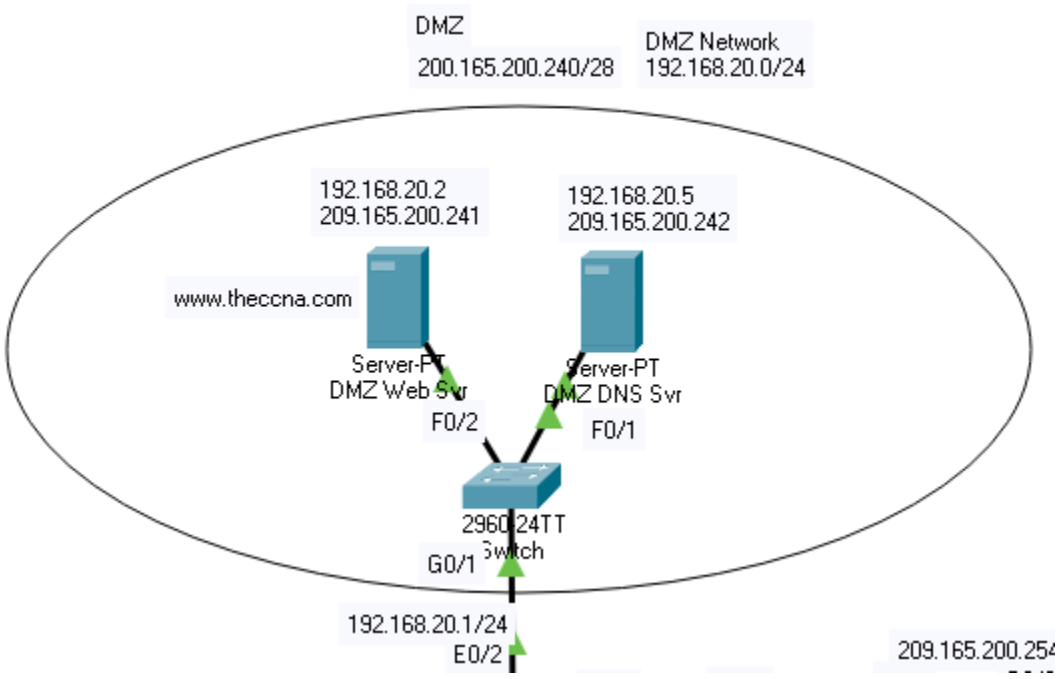
حيث تحتوي الطبقة الأولى وهي الطبقة الأساسية CORE LAYER على سويتشين رئيسيين هما cisco 3650 24P ، أما الطبقة الثانية و هى طبقة الوصول ACCESS LAYER تحتوى على سويتشات cisco 2900 24P و هى التى يتم توصيل الأجهزة الطرفية بها مثل أجهزة الحاسب الآلي و الطابعات والتليفونات الشبكية كما في الصورة السابقة.

٢- الشبكة الفرعية: وهي شبكة تم تصميمها بالمبنى الفرعي للجامعة بينبع وتحتوى على روتر CISCO ASA 5505 وسويتش ليتمكن العاملون والطلاب من الوصول إلى خوادم شبكة المبنى الرئيسي للجامعة للإستفادة من خدمات الموقع وخدمات نقل الملفات، وقد تم إنشاء شبكة إفتراضية خاصة VPN بين المبنى الرئيسي والفرعي وذلك حتى نتمكن من الوصول إلى موارد الشبكة الوسطية DMZ بالجامعة بأمان وخصوصية



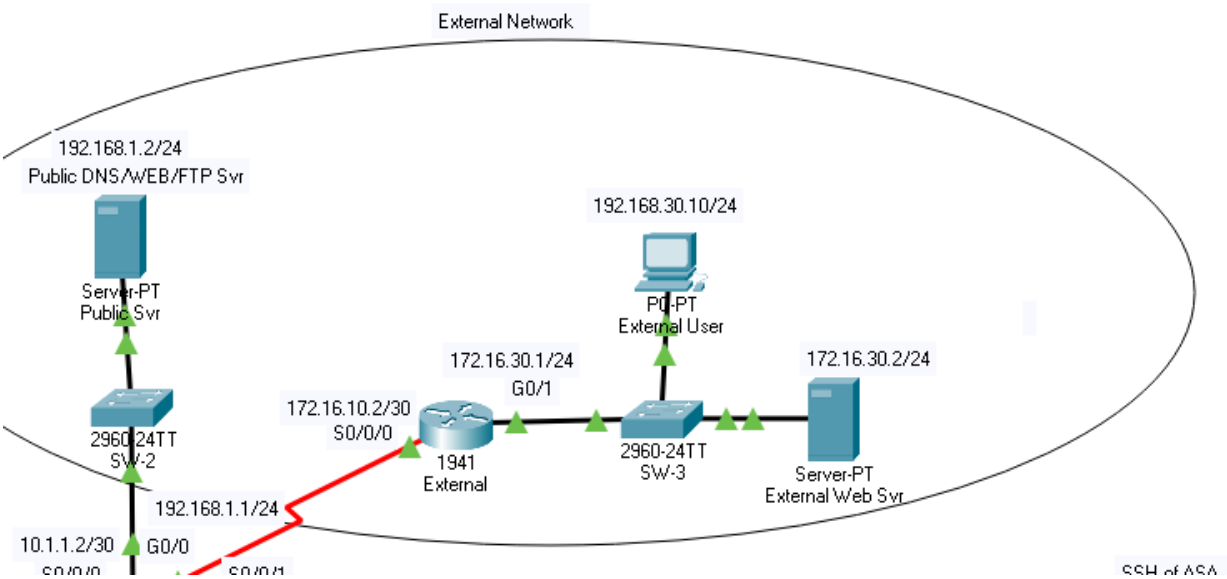
٣- شبكة DMZ (Demilitarized Zone)

وهي شبكة وسطية يتم فيها وضع الخوادم التى يحتاج المستخدمون الوصول إليها من الشبكة الداخلية للجامعة أو من خارج الجامعة مثل فروع الجامعة المنتشرة فى مواقع جغرافية أو للمستخدمون فى منازلهم، وقد تم وضع هذه الخوادم فى شبكة بعيدة عن الشبكة الداخلية وذلك لكونها مواجهه للإنترنت وما يمكن أن تتعرض له من هجمات وإختراقات



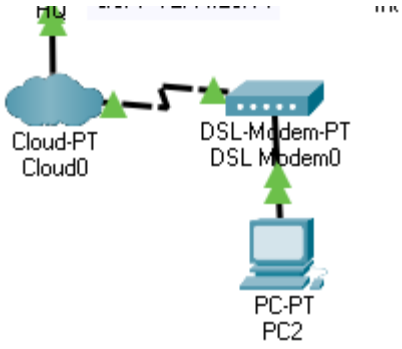
٤- الشبكة الخارجية :

وهى تُعبِّر عن شبكة الإنترنت حول العالم وبها موقع خارجي
(172.16.30.2) www.external.com وكذلك خادم اسم النطاق DNS
(192.168.1.2) server به سجل للموقع السابق ذكره و الموقع الداخلي
(209.165.200.241 – 192.168.20.2) www.theccna.com



٥- شبكة الإتصال عن بعد

وهي عبارة عن جهاز حاسب آلى موجود فى منزل على سبيل المثال وتم توصيله بالإنترنت عن طريق موديم عادى منزلي وذلك لتجربة الشبكة الافتراضية الخاصة التى تم إعدادها على الراوتر الرئيسي للجامعة مخصصاً لمنسوبي الجامعة الذين يريدون الوصول إلى الشبكة الوسطية بالجامعة DMZ من منازلهم أو مواقع جغرافية أخرى على الكوكب



عناوين الأجهزة (IP ADDRESSING)

بالنسبة للشبكة الداخلية فقد تم تقسيم عناوينها كالتالى

عنوان الشبكة	قناع الشبكة	الشبكة الافتراضية (Vlan)	عنوان البوابة الإفتراضية	عنوان بروتوكول جهاز التوجيه السريع الاستعداد (HSRP IP)	
				السويتش الرئيسى الأول CORE 1	السويتش الرئيسى الثانى CORE 2
192.168.10.0	255.255.255.0	1	192.168.10.1	192.168.10.253	192.168.10.254
192.168.100.0	255.255.255.0	10	192.168.100.1	192.168.100.253	192.168.100.254
192.168.200.0	255.255.255.0	20	192.168.200.1	192.168.200.253	192.168.200.254
192.168.250.0	255.255.255.0	30	192.168.250.1	192.168.250.253	192.168.250.254

	الجهاز		العنوان	القناع	البوابة الإفتراضية
DMZ	منفذ ال ASA		192.168.20.1	255.255.255.0	209.165.200.254
	خادم الويب www.theccna.com		192.168.20.2	255.255.255.0	192.168.20.1
	DNS		192.168.20.5	255.255.255.0	192.168.20.1
الشبكة الداخلية	خادم NTP		192.168.10.10	255.255.255.0	192.168.10.1
	السويتش الرئيسى الأول CORE 1	Vlan 1	192.168.10.251	255.255.255.0	192.168.10.1
		Vlan 2	192.168.100.251	255.255.255.0	192.168.10.1
		Vlan 3	192.168.200.251	255.255.255.0	192.168.10.1
		Vlan 30	192.168.250.251	255.255.255.0	192.168.10.1
	السويتش الرئيسى الثانى CORE 2	Vlan 1	192.168.10.252	255.255.255.0	192.168.10.1
		Vlan 10	192.168.100.252	255.255.255.0	192.168.10.1
		Vlan 20	192.168.200.252	255.255.255.0	192.168.10.1
		Vlan 30	192.168.250.252	255.255.255.0	192.168.10.1
	منفذ ال ASA		192.168.20.1	255.255.255.0	209.165.200.254
	منفذ ال ASA		209.165.200.253	255.255.255.0	209.165.200.254
	روتر المبنى الرئيسى		209.165.200.254	255.255.255.0	10.1.1.2
الشبكة الخارجية			10.1.1.1	255.255.255.0	10.1.1.2
شبكة الإتصال عن بعد			72.44.20.14	255.255.255.0	10.1.1.2
	حاسب ألى الإتصال عن بعد		72.44.20.1	255.255.255.0	72.44.20.14
الشبكة الفرعية بينبع	حاسب ألى بفرع ينبع		172.16.40.10	255.255.255.0	172.16.40.1
	روتر فرع ينبع		172.16.40.1	255.255.255.0	172.16.20.1

تنفيذ أهداف المشروع

ما هى تقنية ال VPN

تمد الشبكة الافتراضية الخاصة (VPN) شبكة خاصة عبر شبكة عامة وتمكن المستخدمين من إرسال واستقبال البيانات عبر الشبكات المشتركة أو العامة كما لو كانت أجهزة الحوسبة الخاصة بهم متصلة مباشرة بالشبكة الخاصة.

تشمل مزايا VPN زيادة في الوظائف والأمان وإدارة الشبكة الخاصة.

توفر الوصول إلى الموارد التي يتعذر الوصول إليها على الشبكة العامة ويستخدم عادة للعاملين عن بعد. التشفير شائع ، على الرغم من أنه ليس جزءًا متأصلًا في اتصال VPN.

يتم إنشاء VPN من خلال إنشاء اتصال افتراضي من نقطة إلى نقطة من خلال استخدام دوائر مخصصة أو مع بروتوكولات الأنفاق عبر الشبكات الحالية.

يمكن أن توفر VPN المتوفرة من الإنترنت العام بعض مزايا شبكة المنطقة الواسعة (WAN). من منظور المستخدم ، يمكن الوصول إلى الموارد المتاحة داخل الشبكة الخاصة عن بعد.

١- أنواعها :

a. الوصول عن بعد : يعد تكوين مضيف إلى شبكة مماثلاً لتوصيل جهاز كمبيوتر بشبكة اتصال محلية. يوفر هذا النوع الوصول إلى شبكة مؤسسة ، مثل إنترانت. يمكن استخدام هذا للعمال العاملين عن بُعد الذين يحتاجون إلى الوصول إلى الموارد الخاصة ، أو لتمكين العامل المتنقل من الوصول إلى الأدوات المهمة دون تعريضها للإنترنت العام.
تستخدم الشركات شبكات VPN للوصول عن بُعد لإنشاء اتصال آمن بين شبكتها والأجهزة التي يستخدمها العمال عن بُعد.

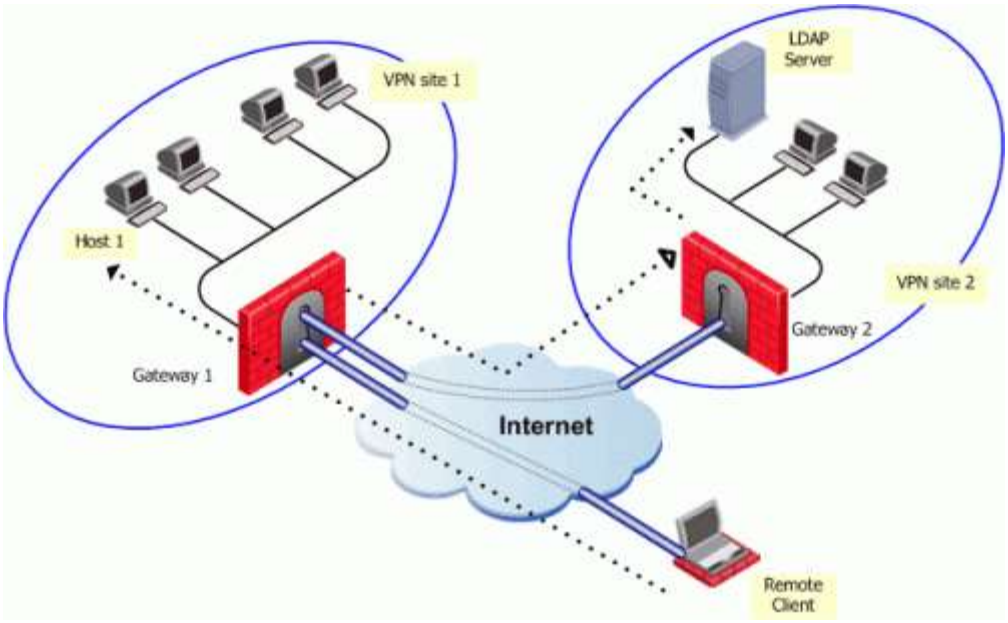
بمجرد الاتصال ، يمكن للموظفين الوصول إلى الموارد الموجودة على الشبكة تمامًا كما لو تم توصيل أجهزتهم فعليًا بالمكتب.

تعمل شبكة VPN للوصول عن بُعد من خلال إنشاء نفق افتراضي بين جهاز الموظف وشبكة الشركة. يمر هذا النفق عبر الإنترنت العام ولكن البيانات المرسلة ذهابًا وإيابًا من خلاله محمية ببروتوكولات التشفير والأمان للمساعدة في الحفاظ على خصوصيتها وأمانها.

المكونان الرئيسيان لهذا النوع من VPN هما خادم الوصول إلى الشبكة (يُطلق عليه غالبًا NAS ولكن لا يجب الخلط بينه وبين التخزين المتصل بالشبكة) وبرنامج عميل VPN.

قد يكون خادم الوصول إلى الشبكة خادمًا مخصصًا أو قد يكون تطبيقًا برمجيًا يعمل على خادم مشترك. يتصل المستخدمون بـ NAS عبر الإنترنت من أجل استخدام VPN للوصول عن بُعد. لتسجيل الدخول إلى VPN ، يتطلب NAS أن يقدم المستخدمون بيانات اعتماد صالحة. لمصادقة بيانات الاعتماد هذه ، يستخدم NAS إما عملية المصادقة الخاصة به أو خادم مصادقة منفصل يعمل على الشبكة.

يجب على المستخدمين أيضًا تثبيت برنامج العميل على أجهزتهم لإنشاء اتصال بشبكة VPN والحفاظ عليه. تأتي معظم أنظمة التشغيل اليوم مزودة ببرامج مدمجة يمكنها الاتصال بشبكة VPN للوصول عن بُعد ، على الرغم من أن بعض خدمات VPN قد تتطلب من المستخدمين تثبيت تطبيق معين بدلاً من ذلك. يقوم برنامج العميل بإعداد الاتصال النفقي بـ NAS ويدير التشفير المطلوب للحفاظ على الاتصال آمنًا.



الفائدة الأكثر أهمية هي أمن البيانات. عندما يرسل موظف خارج الموقع البيانات عبر VPN ، يتم تشفيرها ، لذلك حتى إذا كان المتسلل قادرًا على اعتراض تلك البيانات ، فلن يتمكن من استخدامها. هذا مهم بشكل خاص إذا وصل الموظف إلى شبكة شركاته باستخدام شبكة Wi-Fi عامة أثناء السفر لأن حركة المرور المرسلة عبر هذه الشبكات لا تكون مشفرة عادةً.

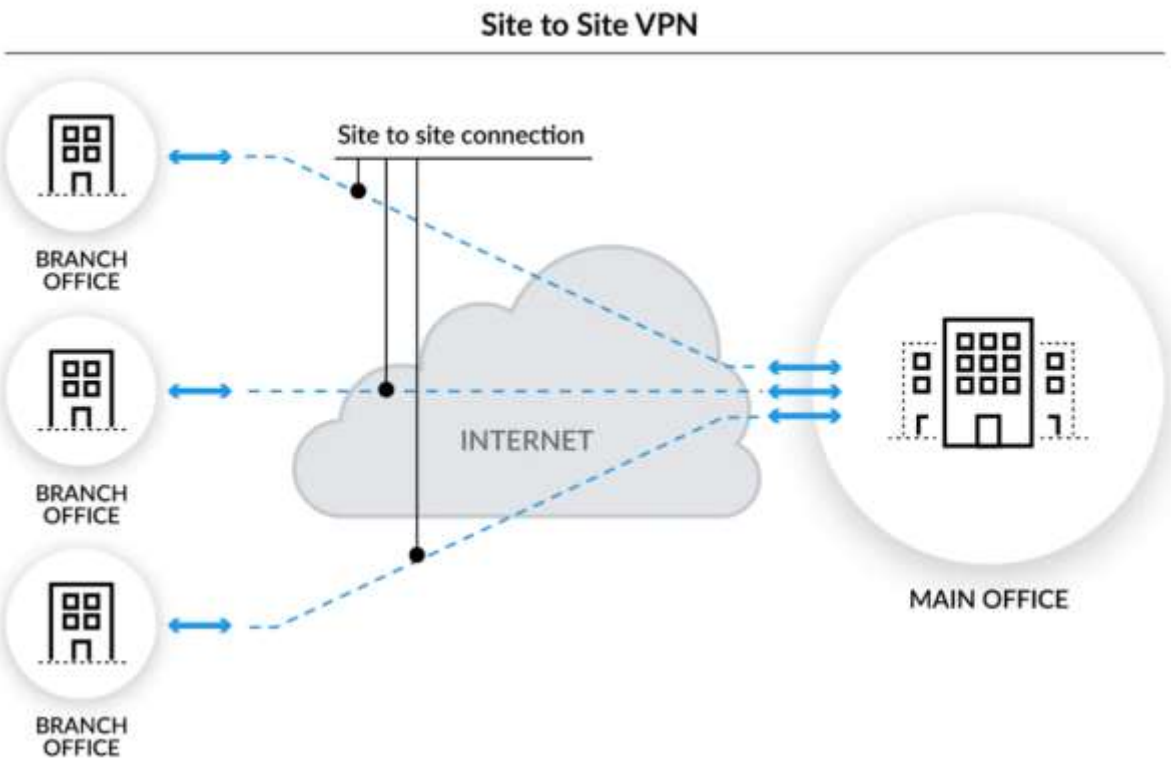
ميزة أخرى لشبكات VPN للوصول عن بعد هي أنها توفر للشركات طريقة قليلة التكلفة لتأمين البيانات التي يرسلها الموظفون خارج الموقع. الاستثمار الأولي اللازم لإعداد VPN للوصول عن بعد ضئيل ويمكن بسهولة توسيع نطاقها مع نمو الشركة وهذا صحيح بشكل خاص إذا تم استخدام مزود خدمة VPN.

نظرًا لأن شبكات VPN للوصول عن بُعد قليلة التكلفة وآمنة، يمكن للمؤسسات أن تشعر براحة أكبر في السماح لموظفيها بالعمل من

المنزل أو أثناء السفر. يميل الموظفون الذين يمكنهم العمل أينما ومتى يريدون أن يكونوا أكثر سعادة وإنتاجية.

b. من موقع لاخر : تكوين موقع إلى موقع يربط شبكتين. يقوم هذا التكوين بتوسيع شبكة عبر مكاتب متباينة جغرافيًا ، أو مجموعة من المكاتب لتثبيت مركز البيانات. قد يعمل ارتباط التوصيل البيني عبر شبكة وسيطة غير متشابهة ، مثل شبكتي IPv6 متصلتين عبر شبكة IPv4.
استخدمت الشركات تقليديًا شبكات VPN من موقع إلى موقع لربط شبكة الشركة الخاصة بها والمكاتب الفرعية البعيدة في طوبولوجيا المحور والتحدث hub-and-spoke topology . يعمل هذا النهج عندما يكون لدى الشركة مركز بيانات داخلي أو تطبيقات شديدة الحساسية أو متطلبات الحد الأدنى من النطاق الترددي. ومع ذلك ، الآن بعد أن نقلت معظم الشركات تطبيقاتها وبياناتها إلى السحابة

ولديها قوى عاملة متنقلة كبيرة ، لم يعد من المنطقي أن يضطر المستخدمون إلى المرور عبر مركز بيانات داخلي للوصول إلى السحابة عندما يمكنهم بدلاً من ذلك الانتقال إلى السحابة مباشرة.
وبالتالي ، تحتاج الشركات إلى إعداد طوبولوجيا الشبكة مع الوصول إلى تطبيقات السحابة أو مركز البيانات. هذا يقود المؤسسات إلى إعداد بنى للشبكات لا تعتمد على إعادة كل حركة المرور إلى المقر الرئيسي.



٢- آليات الأمن : يمكن لشبكات VPN أن تجعل الاتصالات عبر الإنترنت مجهولة تمامًا ، ولكن يمكنها عادةً زيادة الخصوصية والأمان.
لمنع الكشف عن المعلومات الخاصة ، تسمح شبكات VPN عادةً بالوصول عن بُعد المصادق عليه فقط باستخدام بروتوكولات الأنفاق وتقنيات التشفير. يوفر نموذج أمان VPN:

a. السرية مثل أنه حتى إذا تم شم حركة مرور الشبكة على مستوى الحزمة (انظر شم الشبكة والفحص العميق للحزم) ، فلن يرى المهاجم سوى البيانات المشفرة
b. مصادقة المرسل لمنع المستخدمين غير المصرح لهم من الوصول إلى VPN

c. سلامة الرسائل لاكتشاف أي حالات تلاعب بالرسائل المرسلة.

تشمل بروتوكولات VPN الآمنة ما يلي:

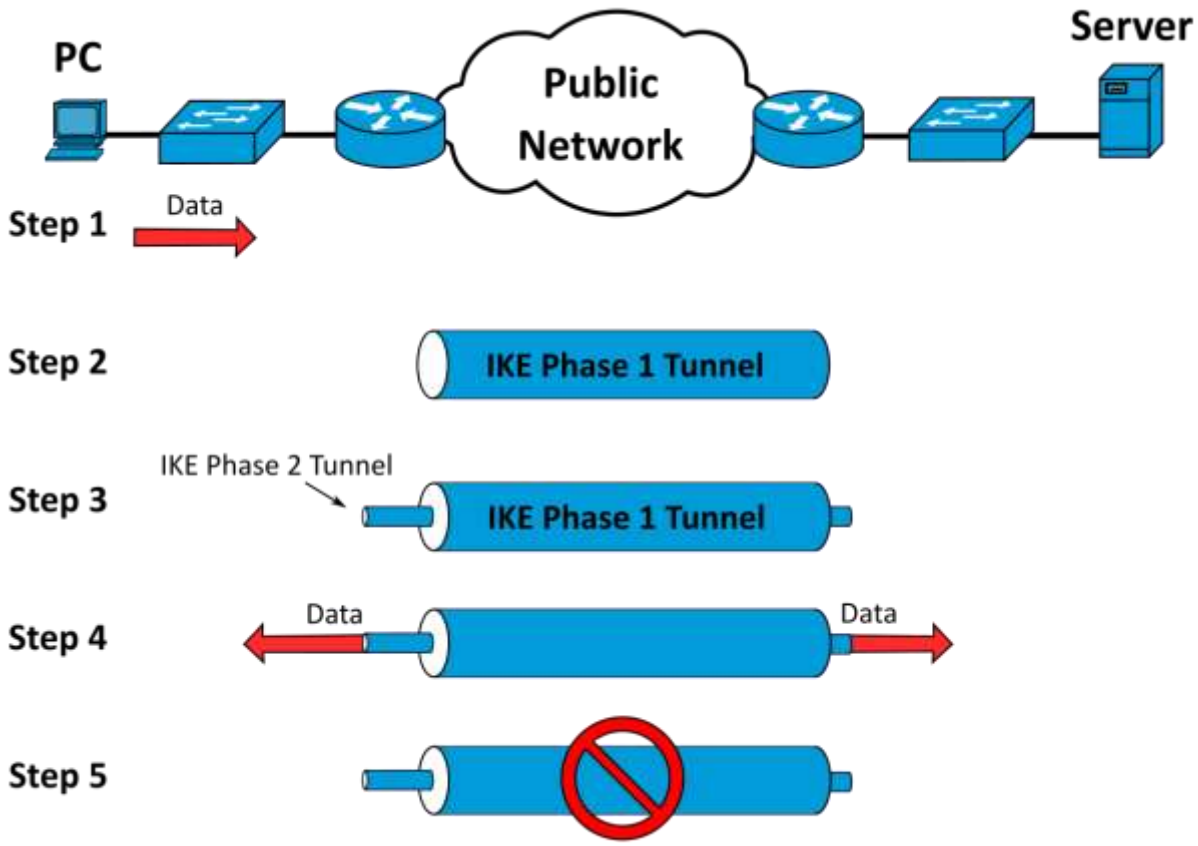
- تم تطوير أمان بروتوكول الإنترنت (IPsec) في البداية بواسطة فريق عمل هندسة الإنترنت (IETF) لـ IPv6 ، والذي كان مطلوبًا في جميع تطبيقات IPv6 المتوافقة مع المعايير قبل أن يقدم RFC 6434 توصية فقط. يستخدم بروتوكول الأمان المستند إلى المعايير أيضًا على نطاق واسع مع IPv4 وبروتوكول Layer 2 Tunneling Protocol. يلبي تصميمه معظم أهداف الأمان: التوافر والنزاهة والسرية. يستخدم IPsec التشفير، وتغليف حزمة IP داخل حزمة IPsec. يحدث إلغاء التغليف في نهاية النفق ، حيث يتم فك تشفير حزمة IP الأصلية وإعادة توجيهها إلى وجهتها المقصودة.
- يمكن لـ Transport Layer Security (SSL / TLS) نقل حركة مرور الشبكة بالكامل (كما هو الحال في مشروع Open VPN) أو تأمين اتصال فردي. يوفر عدد من البائعين إمكانات VPN للوصول عن بُعد من خلال SSL. يمكن لـ SSL VPN الاتصال من المواقع التي تواجه فيها IPsec مشاكل مع ترجمة عنوان الشبكة وقواعد جدار الحماية.
- أمان طبقة نقل مخطط البيانات (DTLS) - يُستخدم في Cisco AnyConnect VPN وفي Open Connect VPN لحل المشكلات التي يواجهها SSL / TLS مع النفق عبر TCP (يمكن أن يؤدي نفق TCP عبر TCP إلى تأخيرات كبيرة وإحباط اتصال).
- يعمل Microsoft Point-to-Point Encryption (MPPE) مع بروتوكول الاتصال النفقي من نقطة إلى نقطة وفي العديد من التطبيقات المتوافقة على الأنظمة الأساسية الأخرى.
- أنفاق بروتوكول Microsoft Secure Socket Tunneling Protocol (SSTP) بروتوكول نقطة إلى نقطة (PPP) أو بروتوكول

Layer 2 Tunneling Protocol عبر قناة SSL / TLS (تم تقديم SSTP في Windows Server 2008 و Windows Vista Service Pack 1).

- شبكة خاصة افتراضية متعددة المسارات (MPVPN). تمتلك شركة Ragula Systems Development Company العلامة التجارية المسجلة "MPVPN".
- Secure Shell (SSH) VPN - يوفر OpenSSH نفق VPN (يختلف عن إعادة توجيه المنفذ) لتأمين الاتصالات عن بُعد بشبكة أو إلى ارتباطات بين الشبكات. يوفر خادم OpenSSH عددًا محدودًا من الأنفاق المتزامنة. ميزة VPN نفسها لا تدعم المصادقة الشخصية.
- Wire Guard هو بروتوكول. في عام ٢٠٢٠، تمت إضافة دعم Wire Guard إلى كل من نواة Linux [١٤] و Android[١٥]، مما فتح المجال للاعتماد من قِبل موفري VPN. بشكل افتراضي، يستخدم Wire Guard Curve25519 لتبادل المفاتيح و ChaCha20 للتشفير، ولكنه يتضمن أيضًا القدرة على مشاركة مفتاح متماثل مسبقًا بين العميل والخادم.
- IKEv2 هو اختصار يرمز إلى مجلد تبادل مفتاح الإنترنت ٢. تم إنشاؤه بواسطة Microsoft و Ciscoويستخدم جنبًا إلى جنب مع IPsec للتشفير والمصادقة. يتم استخدامه الأساسي في الأجهزة المحمولة ، سواء على شبكات G٣ أو G LTE٤ ، لأنه فعال في إعادة الانضمام عند فقد الاتصال.

٣- المصادقة

يجب مصادقة نقاط نهاية النفق قبل التمكن من إنشاء أنفاق VPN آمنة. قد تستخدم شبكات VPN التي يتم الوصول إليها عن بُعد والتي ينشئها المستخدم كلمات مرور أو مقاييس حيوية أو مصادقة ثنائية أو طرق تشفير أخرى. غالبًا ما



تستخدم أنفاق الشبكة إلى الشبكة كلمات مرور أو شهادات رقمية. يقومون بتخزين المفتاح بشكل دائم للسماح للنفق بالتأسيس تلقائيًا ، دون تدخل من المسؤول.

تفاصيل عن ال IPSEC

في مجال الحوسبة ، يعد Internet Protocol Security (IPsec) مجموعة بروتوكولات شبكة آمنة تقوم بمصادقة حزم البيانات وتشفيرها لتوفير اتصال آمن مشفر بين جهازي كمبيوتر عبر شبكة بروتوكول الإنترنت. يتم استخدامه في الشبكات الخاصة الافتراضية (VPN).

يتضمن IPsec بروتوكولات لتأسيس مصادقة متبادلة بين الوكلاء في بداية الجلسة والتفاوض على مفاتيح التشفير لاستخدامها أثناء الجلسة. يمكن لـ IPsec حماية تدفقات البيانات بين زوج من المضيفين (مضيف إلى مضيف) ، بين زوج من بوابات الأمان (شبكة إلى شبكة) ، أو بين بوابة أمان ومضيف (شبكة إلى مضيف).

يستخدم IPsec خدمات الأمان المشفرة لحماية الاتصالات عبر شبكات بروتوكول الإنترنت (IP). وهو يدعم مصادقة الأقران على مستوى الشبكة ، ومصادقة أصل البيانات ، وسلامة البيانات ، وسرية البيانات (التشفير) ، وحماية إعادة التشغيل.

تم تطوير مجموعة IPv4 الأولية بشروط أمنية قليلة. كجزء من تحسين IPv4 ، يعتبر IPsec نموذج طبقة ٣ OSI أو نظام أمان من طرف إلى طرف لطبقة الإنترنت. في المقابل ، بينما تعمل بعض أنظمة أمان الإنترنت الأخرى المستخدمة على نطاق واسع فوق الطبقة ٣ ، مثل بروتوكول أمان طبقة النقل (TLS) الذي يعمل فوق طبقة النقل و Secure Shell (SSH) التي تعمل في طبقة التطبيق ، يمكن لـ IPsec تأمين التطبيقات تلقائيًا في طبقة IP.

هندسة أمن ال IPSEC

IPsec هو معيار مفتوح كجزء من مجموعة IPv4. يستخدم IPsec البروتوكولات التالية لأداء وظائف مختلفة:

- توفر رؤوس المصادقة (AH) تكامل البيانات بدون اتصال ومصادقة أصل البيانات لمخططات بيانات IP وتوفر الحماية ضد هجمات إعادة التشغيل.
- يوفر تغليف حمولات الأمان (ESP) السرية ، وتكامل البيانات بدون اتصال ، ومصادقة مصدر البيانات ، وخدمة منع إعادة التشغيل (شكل من أشكال تكامل التسلسل الجزئي) ، وسرية محدودة لتدفق حركة المرور.
- يوفر Internet Security Association and Key Management Protocol (ISAKMP) إطارًا للمصادقة وتبادل المفاتيح ، مع مواد مفاتيح مصادق عليها فعلية مقدمة إما عن طريق التكوين اليدوي مع المفاتيح

المشتركة مسبقًا ، وتبادل مفتاح الإنترنت (IKE و IKEv2) ، ومفاوضات Kerberized عبر الإنترنت من المفاتيح (KINK) أو سجلات DNS IPSECKEY . الغرض من ذلك هو إنشاء اقترانات الأمان (SA) مع حزمة من الخوارزميات والمعلمات اللازمة لعمليات AH و / أو ESP.

أوضاع IPsec

١- وضع النقل

في وضع النقل ، يتم عادةً تشفير أو مصادقة حمولة حزمة IP فقط. التوجيه سليم ، لأن رأس IP لم يتم تعديله أو تشفيره ؛ ومع ذلك ، عند استخدام رأس المصادقة ، لا يمكن تعديل عناوين IP عن طريق ترجمة عنوان الشبكة ، حيث يؤدي ذلك دائمًا إلى إبطال قيمة التجزئة. يتم دائمًا تأمين طبقات النقل والتطبيق بواسطة تجزئة ، لذلك لا يمكن تعديلها بأي شكل من الأشكال ، على سبيل المثال عن طريق ترجمة أرقام المنافذ.

تم تحديد وسيلة لتغليف رسائل IPsec لاجتياز NAT بواسطة مستندات RFC التي تصف آلية NAT-T.

٢- وضع النفق

في وضع النفق ، يتم تشفير حزمة IP بالكامل والمصادقة عليها. ثم يتم تغليفها في حزمة IP جديدة برأس IP جديد. يتم استخدام وضع النفق لإنشاء شبكات خاصة افتراضية للاتصالات من شبكة إلى شبكة (على سبيل المثال بين أجهزة التوجيه لربط المواقع) ، والاتصالات من مضيف إلى شبكة (مثل وصول المستخدم عن بُعد) واتصالات مضيف إلى مضيف (مثل الدردشة الخاصة).

يدعم وضع النفق اجتياز NAT.

الإحتياج إلى الجدار النارى CISCO ASA

في مجال الحوسبة ، يعد جدار الحماية نظام أمان للشبكة يراقب ويتحكم في حركة مرور الشبكة الواردة والصادرة بناءً على قواعد أمان محددة مسبقًا. يُنشئ جدار الحماية عادةً حاجزًا بين شبكة موثوقة وشبكة غير موثوق بها ، مثل الإنترنت.

إن أجهزة الأمان التكيفية Cisco ASA 5500 Series ، أو ببساطة Cisco ASA ، هي خط Cisco لأجهزة أمان الشبكة التي تم تقديمها في مايو ٢٠٠٥ والتي نجحت في ثلاثة خطوط حالية من منتجات Cisco الشائعة:

١- انتهى بيع Cisco PIX ، التي قدمت وظائف ترجمة عناوين الشبكة وجدار الحماية (NAT) في ٢٨ يوليو ٢٠٠٨.

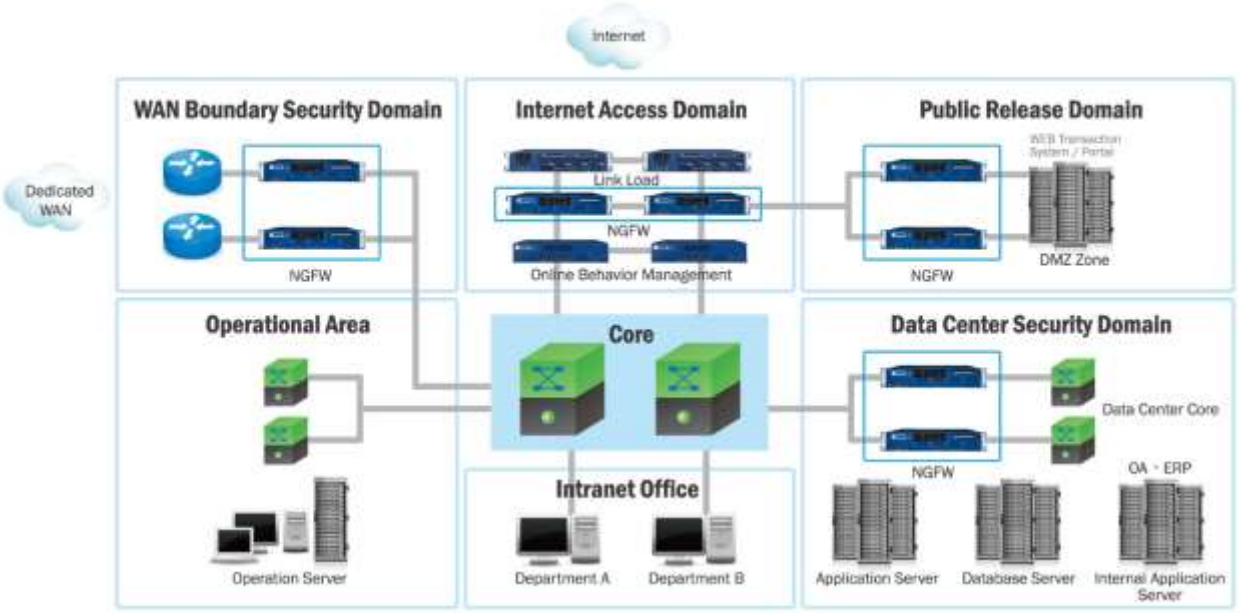
٢- سلسلة Cisco IPS 4200 ، والتي كانت بمثابة أنظمة منع التطفل (IPS).

Cisco VPN 3000 Series Concentrators ، التي توفر شبكات افتراضية خاصة (VPN).

٣- Cisco ASA هو جهاز موحد لإدارة التهديدات ، يجمع بين عدة وظائف أمان للشبكات في صندوق واحد.

يعد جدار الحماية من الجيل التالي (NGFW) جزءًا من الجيل الثالث من تقنية جدار الحماية ، حيث يجمع بين جدار الحماية التقليدي ووظائف تصفية أجهزة الشبكة الأخرى ، مثل جدار حماية التطبيق الذي يستخدم فحص الحزمة العميق المتضمن (DPI) ، وهو نظام منع التطفل (IPS). يمكن أيضًا استخدام تقنيات أخرى ، مثل فحص حركة المرور المشفرة SSL / TLS ، وتصفية مواقع الويب ، وإدارة QoS / النطاق الترددي ، وفحص مكافحة الفيروسات ، وتكامل إدارة هوية الطرف

الثالث (مثل LDAP و RADIUS و Active Directory).



أصبح Cisco ASA أحد أكثر حلول VPN جدار الحماية استخدامًا للشركات الصغيرة والمتوسطة.

وقد أشارت المراجعات المبكرة إلى عدم وجود أدوات Cisco GUI لإدارة الجهاز.

تم تحديد ثغرة أمنية عندما قام المستخدمون بتخصيص خيار Clientless SSL VPN الخاص بـ ASA ولكن تم تصحيحه في عام ٢٠١٥.

تم إصلاح عيب آخر في ميزة WebVPN في عام ٢٠١٨.

يعتمد برنامج ASA على Linux.

يقوم بتشغيل برنامج تنسيق واحد قابل للتنفيذ وقابل للربط يسمى Lina يقوم هذا بجدولة العمليات الداخلية بدلاً من استخدام مرافق Linux.

في تسلسل التمهيد، يبدأ محمل الإقلاع المسمى ROMMON (شاشة ROM)، ويقوم بتحميل نواة Linux، والتي تقوم بعد ذلك بتحميل lina_monitor، والتي

تقوم بعد ذلك بتحميل Lina. يحتوي ROMMON أيضًا على سطر أوامر يمكن استخدامه لتحميل أو تحديد صور وتكوينات البرامج الأخرى.

تتضمن أسماء ملفات البرامج الثابتة مؤشر إصدار ، وتعني -smp أنها مخصصة لمعالج متعدد متماثل (وبنية ٦٤ بت) ، وتشير الأجزاء المختلفة أيضًا إلى ما إذا كان DES٣ أو AES مدعومين أم لا.

يحتوي برنامج ASA على واجهة مشابهة لبرنامج Cisco IOS على أجهزة التوجيه. توجد واجهة سطر أوامر (CLI) يمكن استخدامها للاستعلام عن تشغيل الجهاز أو تكوينه. في وضع التكوين يتم إدخال بيانات التكوين. التهيئة في البداية في الذاكرة كتكوين قيد التشغيل ولكن عادة ما يتم حفظها في ذاكرة فلاش.

نظام كشف التطفل (IDS) و نظام حماية التطفل (IPS)

هو جهاز أو تطبيق برمجي يراقب شبكة أو أنظمة بحثًا عن نشاط ضار أو انتهاكات للسياسة.

عادةً ما يتم الإبلاغ عن أي نشاط تطفل أو انتهاك إما إلى المسؤول أو يتم جمعه مركزيًا باستخدام نظام إدارة المعلومات والأحداث (SIEM). يجمع نظام SIEM بين المخرجات من مصادر متعددة ويستخدم تقنيات تصفية الإنذارات لتمييز النشاط الضار عن الإنذارات الكاذبة.

تتراوح أنواع IDS في النطاق من أجهزة كمبيوتر فردية إلى شبكات كبيرة.

التصنيفات الأكثر شيوعًا هي أنظمة اكتشاف اختراق الشبكة (NIDS) وأنظمة اكتشاف التسلل المستندة إلى المضيف (HIDS). النظام الذي يراقب ملفات نظام التشغيل المهمة هو مثال على HIDS ، في حين أن النظام الذي يحلل حركة مرور الشبكة الواردة هو مثال على NIDS. من الممكن أيضًا تصنيف IDS من خلال نهج الكشف. أكثر المتغيرات شهرة هي الاكتشاف المستند إلى التوقيع (التعرف على الأنماط السيئة ، مثل البرامج الضارة) والاكتشاف المستند إلى العيوب (اكتشاف

الانحرافات عن نموذج حركة المرور "الجيدة" ، والذي يعتمد غالبًا على التعلم الآلي).

متغير شائع آخر هو الاكتشاف المستند إلى السمعة (التعرف على التهديد المحتمل وفقًا لدرجات السمعة). تتمتع بعض منتجات IDS بالقدرة على الاستجابة لعمليات الاقتحام المكتشفة. عادةً ما يُشار إلى الأنظمة التي تتمتع بقدرات استجابة على أنها نظام منع التطفل. يمكن أن تخدم أنظمة كشف التسلل أيضًا أغراضًا محددة من خلال زيادتها بأدوات مخصصة ، مثل استخدام موضع جذب لجذب حركة المرور الضارة وتمييزها.

مقارنة كشف التطفل (IDS) و نظام حماية التطفل (IPS) بجدران الحماية

على الرغم من أن كلاهما يتعلق بأمان الشبكة ، إلا أن IDS يختلف عن جدار الحماية في أن جدار حماية الشبكة التقليدي (يختلف عن جدار حماية الجيل التالي) يستخدم مجموعة ثابتة من القواعد للسماح باتصالات الشبكة أو رفضها. فهو يمنع ضمنً عمليات التطفل، بافتراض أنه قد تم تحديد مجموعة مناسبة من القواعد. بشكل أساسي ، تحد جدران الحماية من الوصول بين الشبكات لمنع التطفل ولا تشير إلى هجوم من داخل الشبكة.

يصف IDS اقتحامًا مشتبهًا به بمجرد حدوثه ويشير إلى إنذار. يراقب نظام كشف التسلل أيضًا الهجمات التي تنشأ من داخل النظام. يتم تحقيق ذلك تقليديًا عن طريق فحص اتصالات الشبكة ، وتحديد الاستدلال والأنماط (المعروفة غالبًا باسم التوقيعات) لهجمات الكمبيوتر الشائعة ، واتخاذ الإجراءات لتنبيه المشغلين.

يُطلق على النظام الذي ينهي الاتصالات نظام منع التطفل ، ويقوم بالتحكم في الوصول مثل جدار حماية طبقة التطبيق.

يعد الوضع الصحيح لأنظمة الكشف عن التطفل أمرًا بالغ الأهمية ويختلف وفقًا للشبكة. يعد الموضع الأكثر شيوعًا خلف جدار الحماية ، على حافة الشبكة.

توفر هذه الممارسة لـ IDS رؤية عالية لحركة المرور التي تدخل شبكتك ولن تتلقى أي حركة مرور بين المستخدمين على الشبكة. حافة الشبكة هي النقطة التي تتصل فيها الشبكة بالإكسترانت. هناك ممارسة أخرى يمكن تحقيقها في حالة توفر المزيد من الموارد وهي استراتيجية حيث يقوم الفني بوضع معرف IDS الأول الخاص به في أعلى نقطة رؤية واعتمادًا على توفر الموارد ، سيضع آخر في أعلى نقطة تالية ، مع الاستمرار في هذه العملية حتى جميع نقاط شبكة مغطاة.

إذا تم وضع IDS خارج جدار حماية الشبكة ، فسيكون الغرض الرئيسي منه هو الدفاع ضد الضوضاء الصادرة عن الإنترنت ، ولكن الأهم من ذلك ، الدفاع ضد الهجمات الشائعة ، مثل عمليات فحص المنافذ ومخطط الشبكة. IDS في هذا الموضع من شأنه أن يراقب الطبقات من ٤ إلى ٧ من نموذج OSI وسيكون قائمًا على التوقيع. هذه ممارسة مفيدة للغاية ، لأنه بدلاً من إظهار الاختراقات الفعلية للشبكة التي نجحت في تجاوز جدار الحماية ، سيتم عرض محاولات الخروقات التي تقلل من مقدار الإيجابيات الكاذبة. يساعد IDS في هذا الموقف أيضًا في تقليل مقدار الوقت المستغرق لاكتشاف الهجمات الناجحة ضد الشبكة.

في بعض الأحيان ، يتم دمج IDS الذي يحتوي على ميزات أكثر تقدمًا مع جدار حماية حتى تتمكن من اعتراض الهجمات المعقدة التي تدخل الشبكة. تتضمن أمثلة الميزات المتقدمة سياقات أمان متعددة في مستوى التوجيه ووضع الجسر. كل هذا بدوره يقلل من التكلفة والتعقيد التشغيلي.

هناك خيار آخر لوضع IDS داخل الشبكة الفعلية. ستكشف هذه الهجمات أو الأنشطة المشبوهة داخل الشبكة. يمكن أن يتسبب تجاهل الأمان داخل الشبكة في

حدوث العديد من المشكلات ، حيث سيسمح للمستخدمين إما بإحداث مخاطر أمنية أو السماح للمهاجم الذي قام بالفعل باختراق الشبكة بالتجول بحرية. يجعل الأمان المكثف للشبكة الداخلية من الصعب حتى على هؤلاء المتسللين داخل الشبكة المناورة وتصعيد امتيازاتهم.

وفى ما يلى هى إعدادات ال IPS التى تم تنفيذها على الروتر الرئيسى للجامعة لتفعيل خاصية كشف التطفل :

```
ip ips config location ipsdir retries 1
ip ips name iosips
ip ips signature-category
category all
retired true
category ios_ips basic
retired false
```

تقنيات التهرب من أنظمة كشف الإختراقات

هناك عدد من الأساليب التي يستخدمها المهاجمون ، وتعتبر الإجراءات التالية بمثابة إجراءات "بسيطة" يمكن اتخاذها لتجنب أنظمة كشف التسلل:

١- التجزئة: بإرسال حزم مجزأة ، سيكون المهاجم تحت الرادار ويمكنه بسهولة تجاوز قدرة نظام الكشف على اكتشاف توقيع الهجوم.
٢- تجنب الافتراضات: لا يوفر منفذ TCP الذي يستخدمه البروتوكول دائمًا إشارة إلى البروتوكول الذي يتم نقله. على سبيل المثال ، قد يتوقع IDS اكتشاف حصان طروادة على المنفذ ١٢٣٤٥. إذا قام المهاجم بإعادة تكوينه لاستخدام منفذ مختلف ، فقد لا يتمكن IDS من اكتشاف وجود حصان طروادة.
٣- الهجمات المنسقة ذات النطاق الترددي المنخفض: تنسيق المسح بين العديد من المهاجمين (أو الوكلاء) وتخصيص منافذ أو مضيفين مختلفين لمهاجمين مختلفين يجعل من الصعب على IDS ربط الحزم التي تم التقاطها واستنتاج أن فحص الشبكة قيد التقدم.
٤- انتحال العنوان / الوكلاء: يمكن للمهاجمين زيادة صعوبة قدرة مسؤولي الأمان على تحديد مصدر الهجوم باستخدام خوادم وكيل مؤمنة بشكل سيئ أو تم

تكوينها بشكل غير صحيح لصد الهجوم. إذا تم انتحال المصدر وارتد من قبل الخادم ، فإنه يجعل من الصعب جدًا على IDS اكتشاف أصل الهجوم.

٥- التهرب من تغيير النمط: تعتمد أنظمة اكتشاف الهوية بشكل عام على "مطابقة النمط" لاكتشاف أي هجوم. من خلال تغيير البيانات المستخدمة في الهجوم بشكل طفيف ، قد يكون من الممكن تجنب الاكتشاف. على سبيل المثال ، قد يكون خادم بروتوكول الوصول إلى الرسائل عبر الإنترنت (IMAP) عرضة لتجاوز سعة المخزن المؤقت ، ويمكن لـ IDS اكتشاف توقيع الهجوم لعشر أدوات هجوم شائعة. من خلال تعديل الحمولة المرسلة بواسطة الأداة ، بحيث لا تشبه البيانات التي يتوقعها نظام كشف البيانات (IDS) ، قد يكون من الممكن تجنب الاكتشاف.

جدار الحماية المعتمد على منطقة IOS

Zone based Firewall

من التطبيقات الشائعة للشبكة للمكاتب الفرعية والمواقع الصغيرة الأخرى التي تنتمي إلى كيان أكبر أن يكون لديك اتصالان WAN: أحدهما عبارة عن MPLS أو اتصال خاص بشبكة الشركة ، والآخر عبارة عن دائرة إنترنت (غالبًا ما تكون بعض نكهات النطاق العريض) الذي ينقل حركة المرور العامة على الإنترنت بالإضافة إلى أنفاق VPN التي تعمل كنسخة احتياطية لدائرة WAN الخاصة. عادةً ما يتطلب اتصال WAN قدرة توجيه ديناميكية (مثل BGP) ولكن القليل من آليات الأمان نظرًا لأنه يمتد فقط لشبكة خاصة. وعلى العكس من ذلك ، يتطلب الاتصال بالإنترنت تطبيقًا قويًا للسياسة ولكن لا يتطلب توجيهًا ديناميكيًا ؛ الطريق الافتراضي نحو الإنترنت يكفي بشكل عام.

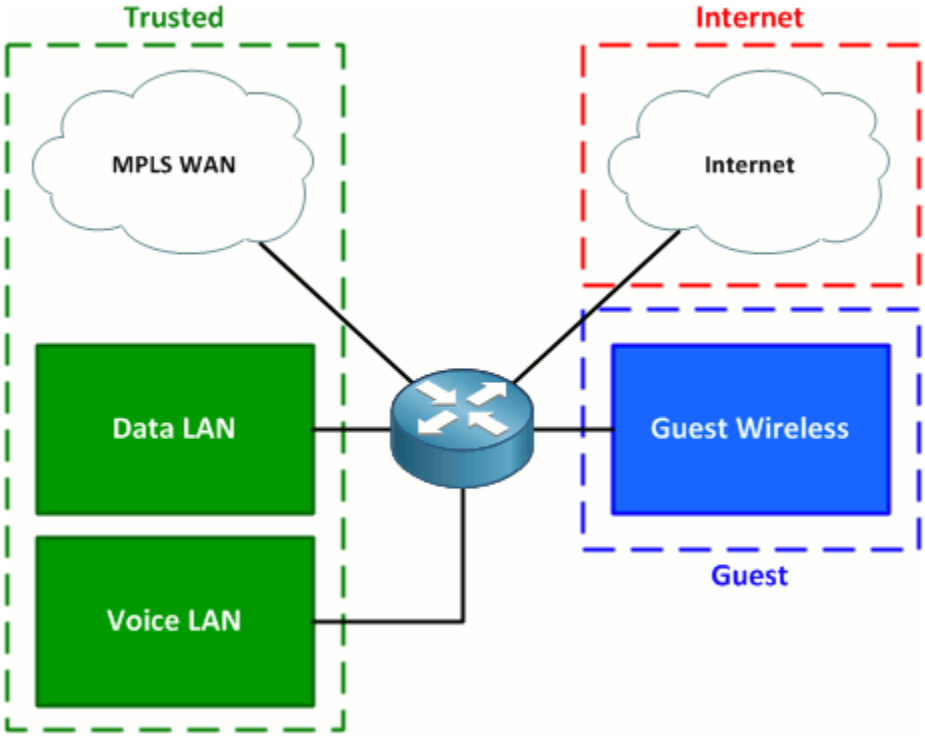
لذلك تختار بعض المؤسسات نشر جهاز مستقل للتعامل مع كل اتصال في مكتب فرعي. ينتهي اتصال MPLS بجهاز توجيه على مستوى الفرع يدعم BGP ويوفر خيارات واجهة مادية مرنة. عادة ما يكون اتصال الإنترنت عبارة عن تسليم إيثرنت

ينتهي بجدار حماية منخفض النهاية. يتم بعد ذلك عادةً توصيل كل من جهاز التوجيه وجدار الحماية بشبكة LAN الداخلية من خلال مفتاح واحد أو أكثر من ثلاثة مفاتيح يعمل على IGP. هذا التصميم عملي ومرن للغاية ، لكن التكلفة الأولية لنشر ثلاثة أجهزة بنية تحتية باهظة الثمن نسبيًا بهذه الطريقة يمكن أن تكون باهظة.

الحل هو نقل وظيفة جدار الحماية إلى جهاز التوجيه ، بحيث تنتهي كلتا الدائرتين في نفس الجهاز. يؤدي هذا إلى إزالة متطلبات جدار الحماية المستقل ومفتاح الطبقة الثالثة ، حيث يقوم جهاز واحد بتنفيذ جميع عمليات التوجيه للموقع. لدعم فرض سياسة الأمان ، سنستخدم ميزة جدار الحماية المستندة إلى المنطقة من Cisco IOS. ملاحظة: تتطلب ميزة جدار الحماية المستند إلى المنطقة ترخيص أمان ورمزًا حديثًا نسبيًا لتعمل بشكل صحيح.

منطقة الأمان Security Zone هي مجموعة من الواجهات الموجهة التي يتم التعامل معها بشكل مشابه من منظور الأمان. على سبيل المثال ، إذا كان لديك اتصالان متكرران بالإنترنت من جهاز توجيه حافة ، فيمكن وضع كلاهما في منطقة مشتركة "غير موثوق بها": وهي غير ذات صلة من منظور الأمان الذي هو الاتصال الأساسي والذي يكون مخصصًا لتجاوز الفشل. ومع ذلك ، سيتم تخصيص اتصال بالشبكة الداخلية إلى منطقة منفصلة وموثوق بها. يمكن أيضًا إنشاء مناطق إضافية بمستويات ثقة قد تقع بين الاثنين ؛ على سبيل المثال ، شبكة لاسلكية ضيف أو شبكة خارجية خاصة بالشركة.

يوضح الهيكل أدناه تصميمًا ينطبق على ما تمت مناقشته أعلاه ، باستخدام ثلاث مناطق أمان متميزة تضم خمسة اتصالات منطقية.



مناطق أمنية Security Zones

تطبق أزواج المناطق تطبيق السياسة على حركة المرور المتدفقة من منطقة أمنية إلى أخرى. يجب تحديد زوج منطقة لكل اتجاه يُسمح فيه ببدء حركة المرور. على سبيل المثال ، تتمثل إحدى السياسات البسيطة الشائعة في أن الشبكة الداخلية يمكنها بدء أي نوع من حركة المرور إلى الإنترنت ، ولكن لا يجوز بدء حركة مرور من الإنترنت إلى الشبكة الداخلية. تتطلب هذه السياسة زوج منطقة واحد فقط ، من المنطقة الداخلية إلى منطقة الإنترنت. إذا كان هناك حاجة لبدء حركة المرور من منطقة الإنترنت إلى المنطقة الداخلية ، فيجب أيضًا إنشاء زوج منطقة ثانٍ (في الاتجاه المعاكس).

في الإصدارات القديمة من جدار الحماية المستند إلى منطقة IOS ، تم السماح لحركة المرور المتدفقة من واجهة إلى أخرى داخل نفس منطقة الأمان بالمرور افتراضيًا. ومع ذلك ، في الإصدارات الحديثة ، حتى حركة المرور داخل المنطقة تتطلب تعريف زوج المنطقة (مع منطقة واحدة كمصدر ووجهة).

جودة الخدمة (QoS)

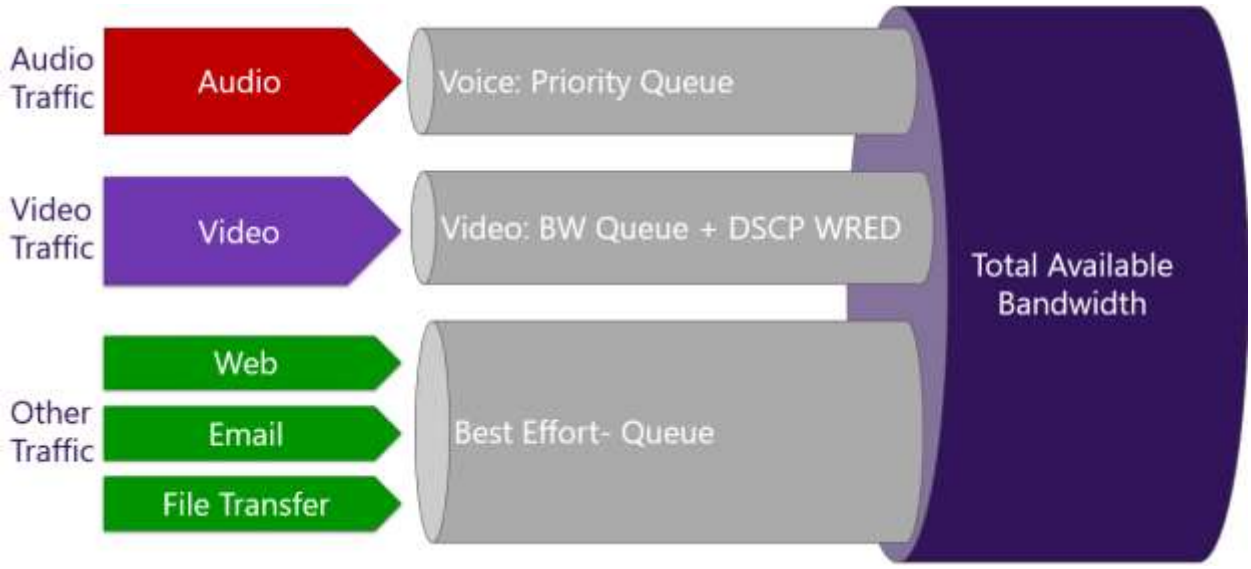
هي وصف أو قياس الأداء العام للخدمة ، مثل الاتصالات الهاتفية أو شبكة الكمبيوتر أو خدمة الحوسبة السحابية ، لا سيما الأداء الذي يراه مستخدمو الشبكة.
لقياس جودة الخدمة كميًا ، غالبًا ما يتم النظر في العديد من الجوانب ذات الصلة بخدمة الشبكة ، مثل فقدان الحزمة ، ومعدل البت bit rate، والإنتاجية ، وتأخير الإرسال ، والتوافر ، والارتعاش ، وما إلى ذلك.

في مجال شبكات الكمبيوتر وشبكات الاتصالات الأخرى ذات الرزم المبدلة ، تشير جودة الخدمة إلى أولويات حركة المرور وآليات التحكم في حجز الموارد بدلاً من جودة الخدمة المحققة. جودة الخدمة هي القدرة على توفير أولويات مختلفة لتطبيقات مختلفة ، أو مستخدمين ، أو تدفقات البيانات ، أو لضمان مستوى معين من الأداء لتدفق البيانات.

جودة الخدمة مهمة بشكل خاص لنقل حركة المرور ذات المتطلبات الخاصة. على وجه الخصوص ، أدخل المطورون تقنية Voice over IP للسماح لشبكات الكمبيوتر بأن تصبح مفيدة مثل شبكات الهاتف للمحادثات الصوتية ، فضلاً عن دعم التطبيقات الجديدة بمتطلبات أداء شبكة أكثر صرامة.

البروتوكولات المستخدمة

توجد العديد من آليات ومخططات جودة الخدمة لشبكات IP.
١- حقل نوع الخدمة (ToS) في عنوان IPv4 (حل محله DiffServ الآن)
٢- الخدمات المميزة (DiffServ)
٣- الخدمات المتكاملة (IntServ)
٤- بروتوكول حجز الموارد (RSVP)
٥- RSVP-TE

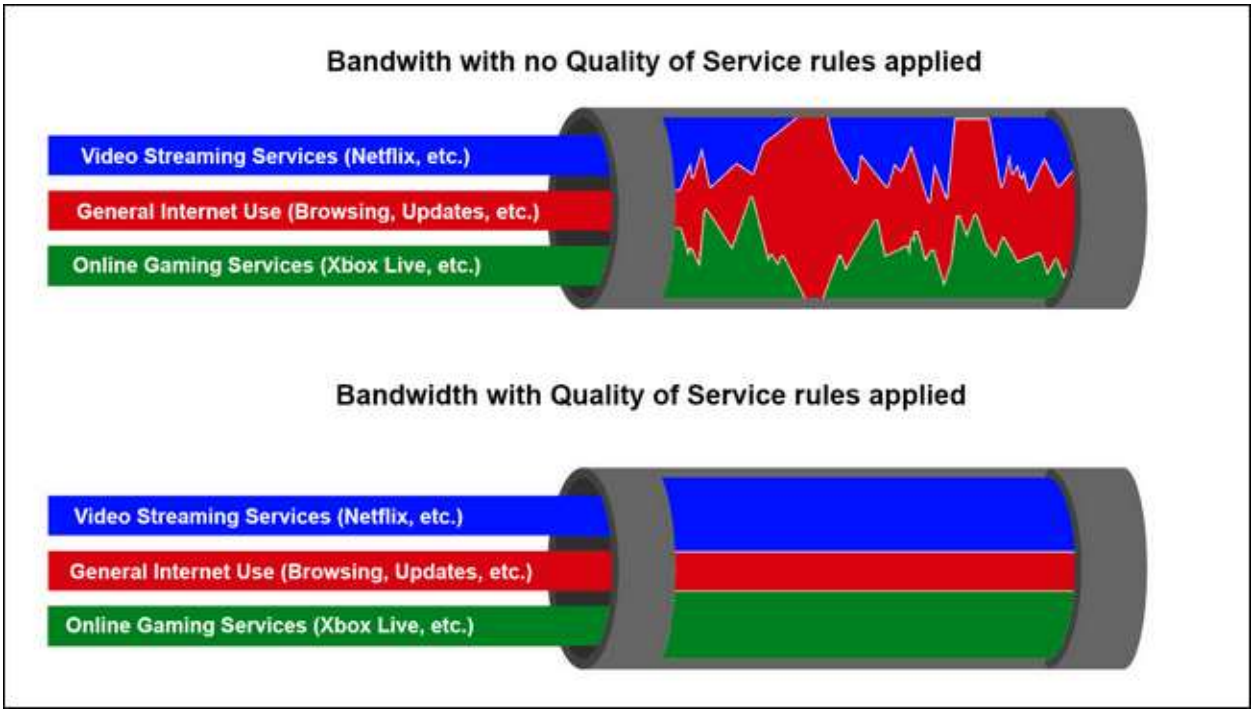


تتوفر إمكانيات QoS في تقنيات الشبكة التالية:

- يوفر تبديل تسمية البروتوكولات المتعددة (MPLS) ثماني فئات QoS
- ترحيل الإطار
- X.25
- بعض أجهزة المودم DSL
- وضع النقل غير المتزامن (ATM)
- يدعم إيثرنت IEEE 802.1Q مع توصيل الصوت والفيديو والشبكات الحساسة للوقت
- تدعم شبكة Wi-Fi معيار IEEE 802.11e
- HomePNA للشبكات المنزلية عبر أسلاك الهاتف والهاتف
- يوفر معيار الشبكات المنزلية G.hn جودة الخدمة عن طريق فرص نقل خالية من الخلاف (CFTXOPs) والتي يتم تخصيصها للتدفقات التي تتطلب جودة الخدمة والتي تفاوضت على عقد مع وحدة تحكم الشبكة. يدعم G.hn أيضًا التشغيل غير QoS عن طريق الفترات الزمنية القائمة على التنازع.

صفات حركة المرور Quality of Traffic

في شبكات تبديل الرزم ، تتأثر جودة الخدمة بعوامل مختلفة يمكن تقسيمها إلى عوامل بشرية وتقنية. تشمل العوامل البشرية: استقرار جودة الخدمة وتوافر الخدمة وأوقات الانتظار ومعلومات المستخدم. تشمل العوامل الفنية: الموثوقية ، وقابلية التوسع ، والفعالية ، وقابلية الصيانة ، وازدحام الشبكة.



يمكن أن تحدث العديد من الأشياء للحزم أثناء انتقالها من الأصل إلى الوجهة ، مما يؤدي إلى المشكلات التالية كما تُرى من وجهة نظر المرسل والمستقبل:

- Goodput

نظرًا للحمل المتفاوت من مستخدمين مختلفين يتشاركون نفس موارد الشبكة ، قد يكون الحد الأقصى للإنتاجية التي يمكن توفيرها لدفق بيانات معين منخفضًا جدًا لخدمات الوسائط المتعددة في الوقت الفعلي.

- فقدان الحزمة

قد تفشل الشبكة في تسليم (إسقاط) بعض الحزم بسبب ازدحام الشبكة. قد يطلب التطبيق المستلم إعادة إرسال هذه المعلومات ، مما قد يؤدي إلى انهيار احتقاني أو تأخيرات غير مقبولة في الإرسال الكلي.

- أخطاء

أحيانًا تكون الحزم تالفة بسبب أخطاء بتات ناتجة عن الضوضاء والتداخل ، خاصة في الاتصالات اللاسلكية والأسلاك النحاسية الطويلة. يجب أن يكتشف المستقبِل ذلك ، وكما لو تم إسقاط الحزمة ، فقد يطلب إعادة إرسال هذه المعلومات.

- وقت الإستجابة

قد يستغرق وصول كل حزمة إلى وجهتها وقتًا طويلاً لأنه يتم تعليقها في طوابير طويلة ، أو أنها تأخذ مسارًا أقل مباشرة لتجنب الازدحام. في بعض الحالات ، قد يؤدي التأخير المفرط إلى جعل تطبيق مثل VoIP أو الألعاب عبر الإنترنت غير قابل للاستخدام.

- اختلاف تأخير الحزمة

ستصل الحزم من المصدر إلى الوجهة بتأخيرات مختلفة. يختلف تأخير الحزمة باختلاف موقعها في قوائم انتظار أجهزة التوجيه على طول المسار بين المصدر والوجهة ، ويمكن أن يختلف هذا الموضع بشكل غير متوقع. يمكن استيعاب اختلاف التأخير في جهاز الاستقبال ، ولكن يؤدي القيام بذلك إلى زيادة زمن الوصول الإجمالي للتيار.

- التسليم خارج الطلب

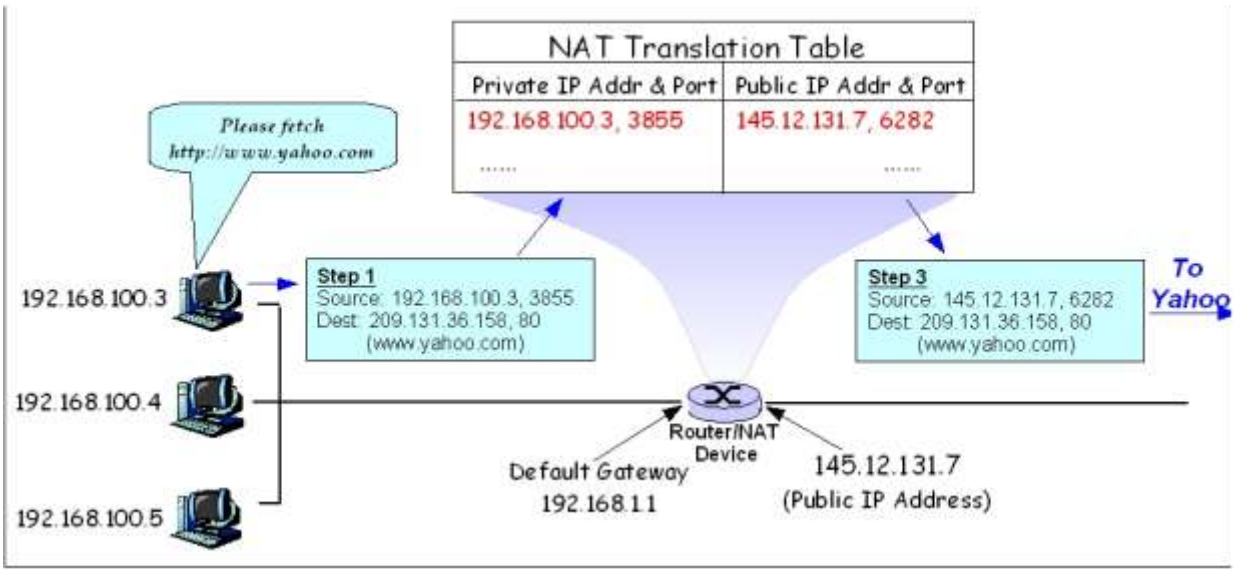
عندما يتم توجيه مجموعة من الحزم ذات الصلة عبر شبكة ، قد تتخذ الحزم المختلفة طرقًا مختلفة ، ينتج عن كل منها تأخير مختلف. والنتيجة هي أن الحزم تصل بترتيب مختلف عما تم إرسالها. تتطلب هذه المشكلة بروتوكولات إضافية خاصة لإعادة ترتيب الحزم خارج الترتيب. تتطلب عملية إعادة الترتيب تخزينًا مؤقتًا

إضافيًا في جهاز الاستقبال ، وكما هو الحال مع اختلاف تأخير الحزمة ، يزيد زمن الانتقال الإجمالي للتيار.

ما هو NAT

ترجمة عنوان الشبكة (NAT) هي طريقة لتعيين مساحة عنوان IP إلى مساحة أخرى عن طريق تعديل معلومات عنوان الشبكة في رأس IP للحزم (IP header) أثناء انتقالها عبر جهاز توجيه حركة المرور.

تم استخدام هذه التقنية في الأصل لتجنب الحاجة إلى تعيين عنوان جديد لكل مضيف عند نقل الشبكة ، أو عند استبدال مزود خدمة الإنترنت المنبع ، ولكن لم يتمكن من توجيه مساحة عناوين الشبكات. لقد أصبح أداة شائعة وأساسية في الحفاظ على مساحة العناوين العالمية في مواجهة استنفاد عناوين IPv4. يمكن استخدام عنوان IP واحد قابل للتوجيه عبر الإنترنت لبوابة NAT لشبكة خاصة كاملة.



نظرًا لأن ترجمة عنوان الشبكة تعدل معلومات عنوان IP في الحزم ، فقد تختلف تطبيقات NAT في سلوكها المحدد في حالات العنونة المختلفة وتأثيرها على حركة مرور الشبكة. لا يتم توثيق تفاصيل سلوك NAT بشكل شائع من قبل بائعي المعدات التي تحتوي على تطبيقات NAT.

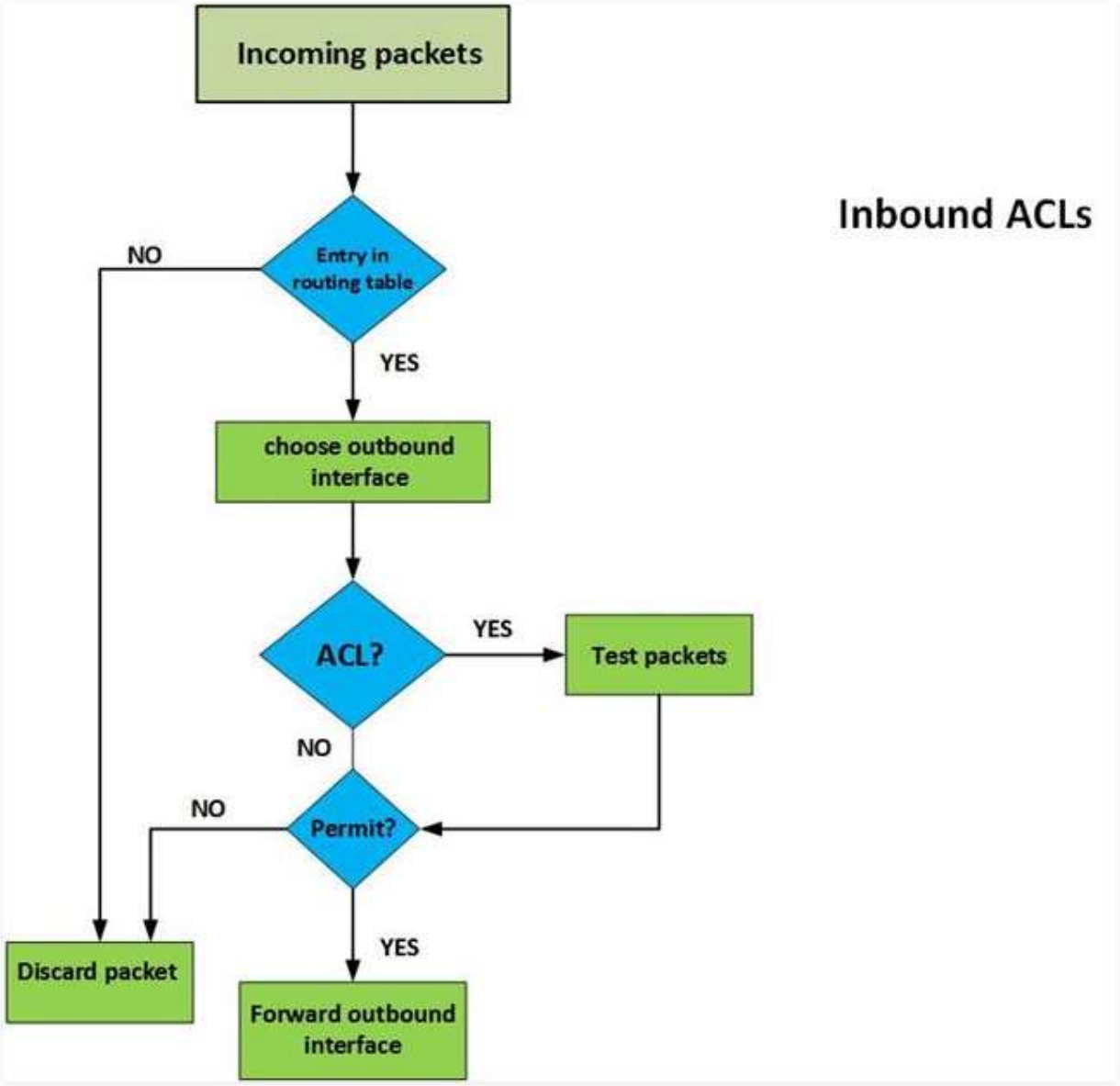
وقد تم إستخدام هذه التقنية فى المشروع هذا لتمكين الشبكة الخاصة الداخلية من الوصول إلى الإنترنت و ذلك بتنفيذ الإعدادات التالية على جهاز cisco ASA

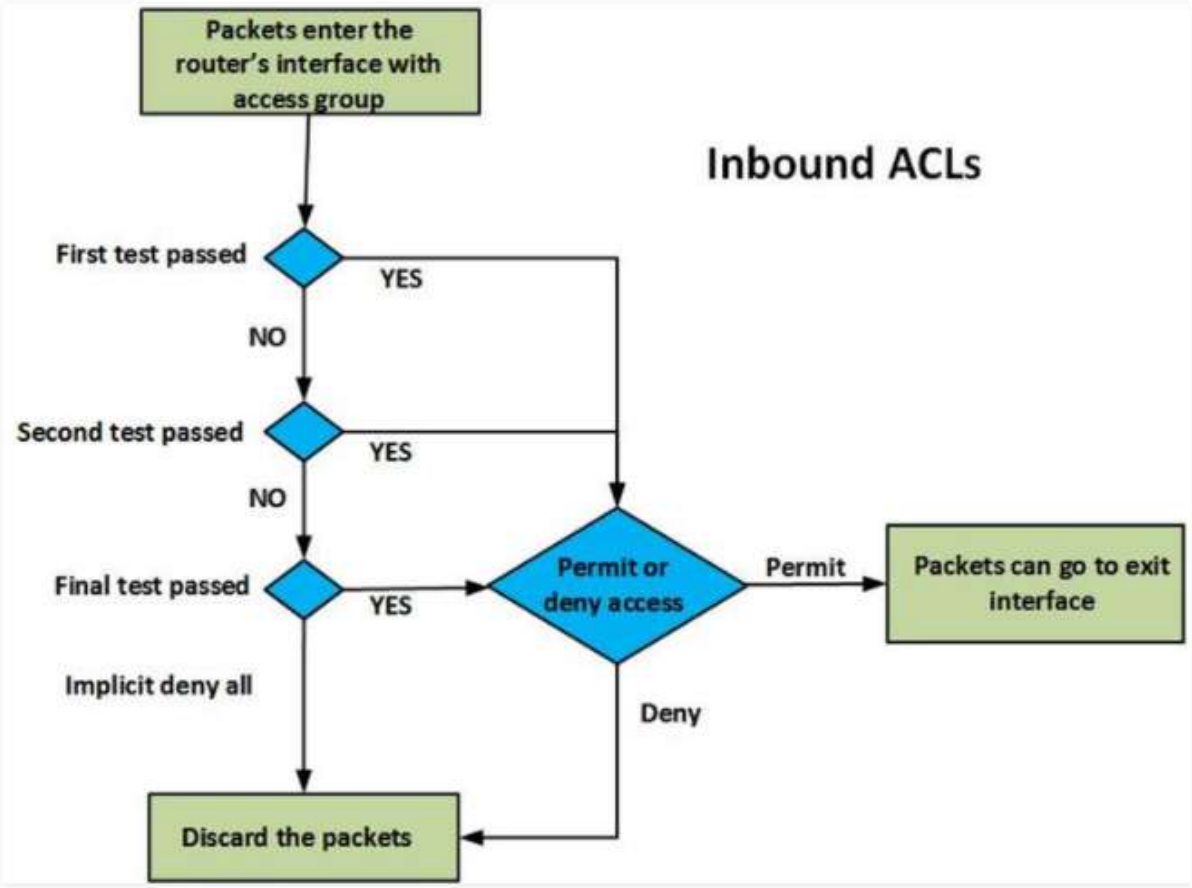
```
access-group OUTSIDE-TO-DMZ in interface outside
object network dmz-dns-server
nat (dmz, outside) static 209.165.200.242
object network dmz-web-server
nat (dmz, outside) static 209.165.200.241
object network inside-nat
nat (inside, outside) dynamic interface
```

قائمة التحكم في الوصول (Access Control List)

هى مجموعة محددة من القواعد المستخدمة لتصفية حركة مرور الشبكة ، خاصة في إعدادات أمان الكمبيوتر. تسمح قوائم ACL بكائنات نظام محددة مثل الأدلة أو الوصول إلى الملفات للمستخدمين المصرح لهم وترفض الوصول إلى المستخدمين غير المصرح لهم.

توجد قوائم ACL بشكل أساسي في أجهزة الشبكة ذات إمكانيات تصفية الحزم بما في ذلك أجهزة التوجيه والمحولات.


Incoming packets
Inbound ACLs
Entry in routing table
NO
YES
choose outbound interface
ACL?
YES
Test packets
NO
Permit?
NO
YES
Discard packet
Forward outbound interface



- كيف تعمل قوائم ACL

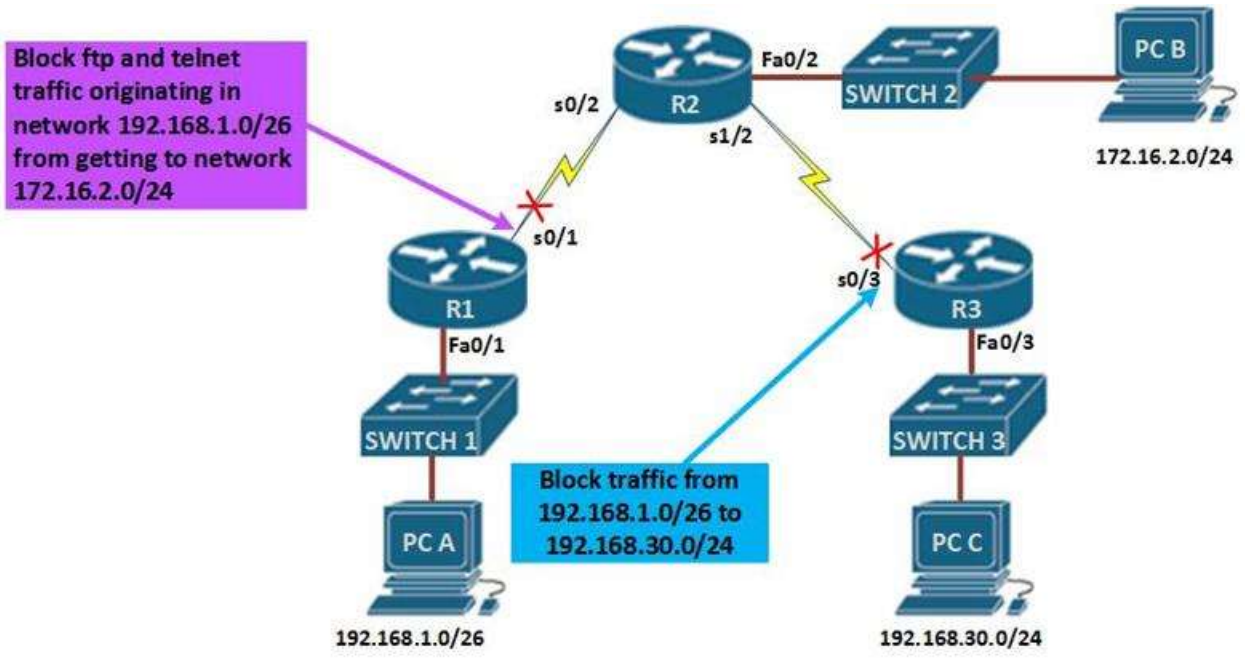
تحتوي قوائم ACL المختلفة على آليات عمل مختلفة بناءً على ما تفعله. بالنسبة لقوائم التحكم في الوصول لنظام الملفات ، فإنها تعمل عن طريق إنشاء جداول تُعلم نظام التشغيل بامتيازات الوصول الممنوحة لموضوعات معينة في النظام. يحتوي كل كائن على خاصية أمان فريدة تعمل كعامل تعريف في قائمة التحكم في الوصول الخاصة به. تتضمن بعض الامتيازات امتيازات القراءة / الكتابة ، وتنفيذ الملف ، والعديد من الامتيازات الأخرى.

تتضمن بعض أنظمة التشغيل الشائعة التي تستخدم هذه الآلية الأنظمة المستندة إلى Unix و Windows NT / 2000 و Novell's Netware.

في حالة شبكات ACLS ، يتم تثبيتها في أجهزة الشبكات (أجهزة التوجيه والمحولات) لغرض وحيد هو تصفية حركة المرور. يتم ذلك باستخدام قواعد محددة مسبقًا تحدد الحزم المنقولة. تلعب عناوين IP المصدر والوجهة أيضًا دورًا رئيسيًا في هذا القرار.

تعمل تصفية الحزم على تحسين أمان الشبكة عن طريق تقليل الوصول إلى حركة مرور الشبكة ، وتقييد وصول الجهاز والمستخدم إلى الشبكة المعنية.

قوائم الوصول ACL متسلسلة ، وتتكون من عنصرين رئيسيين ؛ تصريح التصريحات ورفضها. يتم استخدام اسم ورقم لتعريف قوائم الوصول.



- أنواع قائمة التحكم في الوصول

هناك أربعة أنواع من قوائم ACL التي تلعب أدوارًا مختلفة في الشبكة بما في ذلك ، القياسي ، والانعكاسي ، والممتد ، والديناميكي:

✓ القياسي ACL

يسمح لك هذا النوع بتقييم عناوين IP لمصدر الحزمة فقط. فهي ليست قوية مثل قوائم ACL الممتدة ولكنها تستخدم طاقة حوسبة أقل. يستخدمون أيضًا الأرقام ١٣٠٠-١٩٩٩ أو ١-٩٩ حتى يتمكن جهاز التوجيه من تحديد العنوان المحدد كعنوان IP المصدر.

✓ الممتدACL

تسمح لك هذه الأنواع من قائمة التحكم بالوصول (ACL) بحظر المصدر والوجهة لمضيفين معينين أو الشبكة بأكملها. باستخدام قوائم التحكم في الوصول (ACL) الموسعة ، من الممكن تصفية حركة المرور استنادًا إلى البروتوكولات (IP و TCP و ICMP و UDP).

✓ الانعكاسية ACL

تستخدم قوائم ACL العاكسة ، المعروفة أيضًا باسم قوائم التحكم في الوصول لجلسة IP ، تفاصيل جلسة الطبقة العليا لتصفية حركة المرور.

✓ ديناميكي ACL

كما يوحي المصطلح ، فإن قوائم ACL الديناميكية يمكن الاعتماد عليها في قوائم ACL الممتدة و Telnet والمصادقة. أنها تمنح المستخدمين الوصول إلى مورد فقط إذا كان المستخدم يصادق على الجهاز من خلال مبدأ.

- تطبيقات ACL

لطالما كانت تهديدات الأمن السيبراني في ازدياد ، وقائمة التحكم في الوصول (ACL) هي إحدى الطرق العديدة التي يتم فرضها لحماية الشبكات وجودة الخدمة في المؤسسات. يتم تنفيذ قوائم ACL لحل المشكلات بما في ذلك:

✓ خروقات البيانات للمعلومات السرية

تجاوز عرض النطاق الترددي للشبكة من خلال خدمات غير ذات صلة وبالتالي حرمان الموارد من الخدمات الهامة

✓ الفيروسات والشفرات الخبيثة من دخول المنظمة

تحقق قوائم ACL هدفها الرئيسي من خلال تحديد سلوكيات الوصول إلى الشبكة والتحكم فيها ، والتحكم في تدفق حركة المرور ، والمراقبة الدقيقة.

وفيما يلى تركيبة ال ACL التى تم إعدادها على الروتر الرئيسى للجامعة :

```
access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.241 eq www
access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq domain
access-list OUTSIDE-TO-DMZ extended permit udp any host 209.165.200.242 eq domain
access-list OUTSIDE-TO-DMZ extended permit tcp host 172.16.40.10 host 209.165.200.241 eq ftp
access-list OUTSIDE-TO-DMZ extended permit icmp any any echo
access-list OUTSIDE-TO-DMZ extended permit icmp any any echo-reply
```

مفهوم **الشبكة الافتراضية** VLAN

شبكة LAN الظاهرية (VLAN) هي أي مجال بث مقسم ومعزول في شبكة الكمبيوتر في طبقة ارتباط البيانات (طبقة OSI 2).

LAN هي اختصار لشبكة المنطقة المحلية وفي هذا السياق يشير الظاهري إلى كائن مادي تم إعادة إنشائه وتعديله بواسطة منطق إضافي. تعمل شبكات VLAN من خلال تطبيق العلامات على إطارات الشبكة والتعامل مع هذه العلامات في أنظمة الشبكات - مما يؤدي إلى إنشاء مظهر ووظيفة حركة مرور الشبكة الموجودة فعليًا على شبكة واحدة ولكنها تعمل كما لو كانت مقسمة بين شبكات منفصلة. بهذه الطريقة ، يمكن للشبكات المحلية الظاهرية (VLAN) إبقاء تطبيقات الشبكة

منفصلة على الرغم من اتصالها بنفس الشبكة المادية ، ودون الحاجة إلى نشر مجموعات متعددة من أجهزة الكابلات والشبكات.

تسمح شبكات VLAN لمسؤولي الشبكة بتجميع المضيفين معًا حتى إذا لم يكن المضيفون متصلين مباشرة بمحول الشبكة نفسه. نظرًا لأنه يمكن تكوين عضوية VLAN من خلال البرنامج ، يمكن أن يؤدي ذلك إلى تبسيط تصميم الشبكة ونشرها بشكل كبير. بدون شبكات VLAN ، يحتاج تجميع المضيفين وفقًا لمواردهم إلى العمل على نقل العقد أو إعادة توصيل روابط البيانات. تسمح شبكات VLAN للأجهزة التي يجب أن تبقى منفصلة لمشاركة كبلات شبكة مادية ومع ذلك يتم منعها من التفاعل المباشر مع بعضها البعض. تؤدي هذه المشاركة المُدارة إلى تحقيق مكاسب في البساطة والأمان وإدارة حركة المرور والاقتصاد. على سبيل المثال ، يمكن استخدام شبكة محلية ظاهرية (VLAN) لفصل حركة المرور داخل شركة استنادًا إلى المستخدمين الفرديين أو مجموعات المستخدمين أو أدوارهم (مثل مسؤولي الشبكة) ، أو استنادًا إلى خصائص حركة المرور (مثل حركة المرور ذات الأولوية المنخفضة التي تم منعها من التأثير على بقية أداء الشبكة). تستخدم العديد من خدمات استضافة الإنترنت شبكات VLAN لفصل المناطق الخاصة للعملاء عن بعضها البعض ، مما يسمح بتجميع خوادم كل عميل في قطاع شبكة واحد بغض النظر عن مكان وجود الخوادم الفردية في مركز البيانات. هناك حاجة لبعض الاحتياطات لمنع "الهروب" من حركة المرور من شبكة محلية ظاهرية معينة ، وهي ثغرة تُعرف باسم قفز VLAN.

لتقسيم شبكة إلى شبكات محلية ظاهرية (VLAN) ، يقوم المرء بتكوين معدات الشبكة. قد تقوم المعدات الأكثر بساطة بتقسيم كل منفذ مادي فقط (حتى لو كان كذلك) ، وفي هذه الحالة يتم تشغيل كل شبكة محلية ظاهرية عبر كبل شبكة مخصص. يمكن للأجهزة الأكثر تعقيدًا تحديد الإطارات من خلال علامات VLAN ، بحيث يمكن استخدام اتصال داخلي واحد (جذع) لنقل البيانات لشبكات VLAN متعددة. نظرًا لأن شبكات VLAN تشترك في عرض النطاق الترددي ، يمكن لشبكة

VLAN استخدام تجميع الارتباط أو تحديد أولويات جودة الخدمة أو كليهما لتوجيه البيانات بكفاءة.

مفهوم HSRP

يعد بروتوكول Hot Standby Router (HSRP) بروتوكولًا احتياطيًا مملوكًا لشركة Ciscoلإستخدام بوابة افتراضية حال فشل البوابة الأصلية الفيزياقية . تم وصف الإصدار ١ من البروتوكول في RFC 2281 في عام ١٩٩٨. يتضمن الإصدار ٢ من البروتوكول تحسينات ويدعم IPv6 .

ينشئ البروتوكول ارتباطًا بين العبّارات من أجل تحقيق تجاوز فشل البوابة الافتراضية إذا أصبحت البوابة الأساسية غير قابلة للوصول. ترسل بوابات HSRP رسائل ترحيب متعددة البث *hello* messages إلى البوابات الأخرى لإعلامهم بأولوياتهم (أي البوابة المفضلة) والحالة الحالية (نشطة أو احتياطية).

يعمل جهاز التوجيه الأساسي ذو الأولوية الأعلى كجهاز توجيه افتراضي بعنوان IP للبوابة المحدد مسبقًا وسيستجيب لطلب ARP من الأجهزة المتصلة بالشبكة المحلية باستخدام عنوان MAC الظاهري. إذا فشل جهاز التوجيه الأساسي ، فسيستحوذ جهاز التوجيه ذو الأولوية القصوى التالية على عنوان IP الخاص بالبوابة والإجابة على طلبات ARP بنفس عنوان MAC ، وبالتالي تحقيق تجاوز فشل البوابة الافتراضية.

HSRP ليس بروتوكول توجيه لأنه لا يعلن عن مسارات IP أو يؤثر على جدول التوجيه بأي شكل من الأشكال.

يتمتع HSRP بالقدرة على تشغيل تجاوز الفشل إذا تعطلت واجهة واحدة أو أكثر على جهاز التوجيه. يمكن أن يكون هذا مفيدًا لأجهزة التوجيه ذات الفروع المزدوجة

لكل منها ارتباط واحد يعود بالبوابة. في حالة تعطل ارتباط جهاز التوجيه الأساسي ، سيتولى جهاز التوجيه الاحتياطي الوظيفة الأساسية وبالتالي يحتفظ بالاتصال بالبوابة.

مفهوم EtherChannel

EtherChannel عبارة عن تقنية تجميع أكثر من منفذ تُستخدم بشكل أساسي في محولات Cisco. يسمح بتجميع العديد من ارتباطات Ethernet المادية لإنشاء ارتباط Ethernet منطقي بغرض توفير خاصية تخطى الأخطاء فى حال فشل عمل منفذ، يمكن إنشاء قناة EtherChannel من بين منفذين وثمانية منافذ Fast أو Gigabit أو ١٠-Gigabit Ethernet نشطة ، مع واحد إلى ثمانية منافذ إضافية غير نشطة ، فتصبح نشطة عندما تفشل المنافذ النشطة الأخرى. تُستخدم قناة EtherChannel بشكل أساسي في الشبكة الأساسية ، ولكن يمكن استخدامها أيضًا لتوصيل أجهزة المستخدم النهائي.

اخترع كالبانا تقنية EtherChannel وصممها سكوت تشايلدز الموظف في كالبانا في أوائل التسعينيات. استحوذت شركة Cisco Systems على Kalpana في عام ١٩٩٤. وفي عام ٢٠٠٠ ، اجتاز IEEE معيار ٨٠٢,٣ad ، وهو إصدار قياسي مفتوح من EtherChannel.

مفهوم VTP

بروتوكول (VTP) VLAN هو بروتوكول مملوك لشركة Cisco ينشر تعريف شبكات المنطقة المحلية الظاهرية (VLAN) على شبكة المنطقة المحلية بأكملها. للقيام بذلك ، يحمل VTP معلومات VLAN إلى جميع المحولات في مجال VTP.

يمكن إرسال إعلانات VTP عبر قنوات Q٨٠٢,١ و ISL.

يتوفر VTP في معظم منتجات Cisco Catalyst Family.

باستخدام VTP ، يعلن كل محول عائلي من Catalyst عن ما يلي على منافذ قنوات الاتصال الخاصة به:

١- مجال الإدارة Management domain
٢- رقم مراجعة التكوين Configuration revision number
٣- شبكات VLAN المعروفة ومعلماتها المحددة Known VLANs and their specific parameters

توجد ثلاثة إصدارات من VTP ، وهي الإصدار ١ ، الإصدار ٢ ، الإصدار ٣.

فى أجهزة Cisco ، يحافظ VTP (بروتوكول توصيل VLAN) على اتساق تكوين VLAN عبر شبكة واحدة من الطبقة الثانية. يستخدم VTP إطارات Layer 2 لإدارة إضافة وحذف وإعادة تسمية شبكات VLAN من المحولات في وضع عميل VTP. VTP مسؤول عن مزامنة معلومات VLAN داخل مجال VTP ويقلل من الحاجة إلى تكوين نفس معلومات VLAN على كل محول وبالتالي تقليل احتمالية عدم تناسق التكوين الذي ينشأ عند إجراء التغييرات.

بروتوكول وقت الشبكة (NTP)

هو بروتوكول شبكة لمزامنة الساعة بين أنظمة الكمبيوتر عبر شبكات بيانات ذات زمن انتقال متغير بتبديل الحزم packet-switched, variable-latency data networks. يعمل NTP منذ ما قبل عام ١٩٨٥ ، وهو أحد أقدم بروتوكولات الإنترنت المستخدمة حاليًا. تم تصميم NTP بواسطة David L. Mills من جامعة ديلاوير.

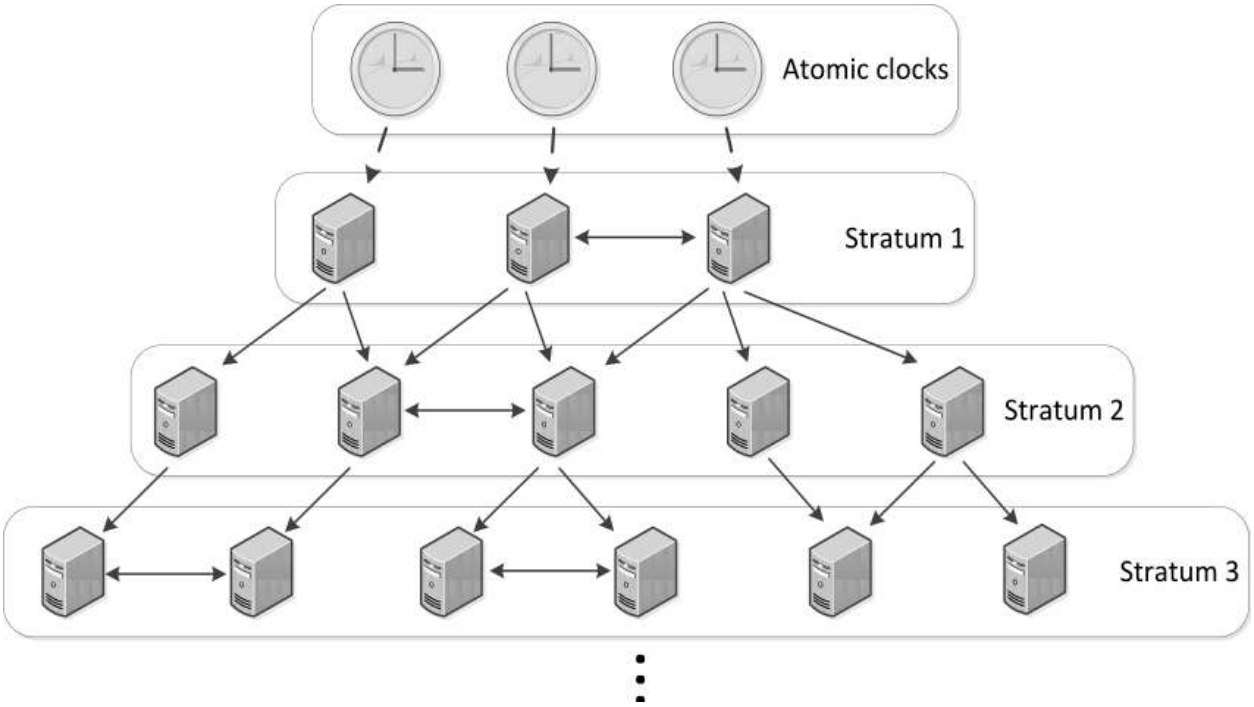
يهدف NTP إلى مزامنة جميع أجهزة الكمبيوتر المشاركة في غضون بضعة أجزاء من الألف من الثانية من التوقيت العالمي المنسق (UTC)

يستخدم خوارزمية التقاطع، وهي نسخة معدلة من خوارزمية Manzullo، لتحديد خوادم الوقت الدقيقة وهي مصممة للتخفيف من تأثيرات زمن الوصول المتغير للشبكة. يمكن أن يحافظ NTP عادةً على الوقت في حدود عشرات المللي ثانية عبر الإنترنت العام ، ويمكن أن يحقق دقة أفضل من ميلي ثانية في شبكات المنطقة المحلية في ظل ظروف مثالية. يمكن أن تتسبب المسارات غير المتماثلة وازدحام الشبكة في حدوث أخطاء تبلغ ١٠٠ مللي ثانية أو أكثر.

عادة ما يتم وصف البروتوكول من حيث نموذج العميل والخادم client–server، ولكن يمكن استخدامه بسهولة في العلاقات من نظير إلى نظير peer-to-peer حيث يعتبر كلا الزملاء peers أن الآخر مصدر زمني محتمل.

ترسل التطبيقات وتستقبل الطوابع الزمنية timestamps باستخدام بروتوكول مخطط بيانات المستخدم (UDP) على المنفذ رقم ١٢٣. يمكنهم أيضًا استخدام البث أو البث المتعدد ، حيث يستمع العملاء بشكل سلبي إلى تحديثات الوقت بعد تبادل معايرة أولي ذهابًا وإيابًا. يوفر NTP تحذيرًا لأي تعديل وشيك للثانية الكبيسة ، ولكن لا يتم إرسال معلومات حول المناطق الزمنية المحلية أو التوقيت الصيفي.

البروتوكول الحالي هو الإصدار ٤ (NTPv4) ، وهو معيار مقترح كما هو موثق في RFC 5905. وهو متوافق مع الإصدارات السابقة مع الإصدار ٣ المحدد في RFC 1305.



المصادقة والترخيص والمحاسبة AAA

يشير AAA إلى المصادقة والترخيص والمحاسبة. يتم استخدامه للإشارة إلى عائلة البروتوكولات التي تتوسط الوصول إلى الشبكة.

نظرًا لأن الوصول عن بُعد يكون متاحًا باستخدام عنوان IP ، فمن الممكن أن يتمكن مستخدم غير مصرح له من الوصول باستخدام عنوان IP نفسه ، وبالتالي ، من أجل تدابير الأمان ، يتعين علينا وضع المصادقة ويجب تشفير الحزم المتبادلة بين الجهاز بحيث لا يتمكن أي شخص آخر من التقاط تلك المعلومات الحساسة.

لذلك، يتم استخدام إطار عمل يسمى AAA لتوفير هذا المستوى الإضافي من الأمان.

AAA هو إطار عمل قائم على المعايير يُستخدم للتحكم في من يُسمح له باستخدام موارد الشبكة (من خلال المصادقة) ، وما هو مصرح له بالقيام به (من خلال التفويض) ، والتقاط الإجراءات التي يتم تنفيذها أثناء الوصول إلى الشبكة (من خلال المحاسبة).

١- المصادقة

العملية التي يمكن من خلالها التعرف على أن المستخدم الذي يريد الوصول إلى موارد الشبكة صحيحة أم لا عن طريق طلب بعض بيانات الاعتماد مثل اسم المستخدم وكلمة المرور. تتمثل الطرق الشائعة في وضع المصادقة على منفذ وحدة التحكم أو منفذ AUX أو خطوط vty.

بصفتنا مسؤولي الشبكة ، يمكننا التحكم في كيفية مصادقة المستخدم إذا أراد شخص ما الوصول إلى الشبكة. تتضمن بعض هذه الطرق استخدام قاعدة البيانات المحلية لهذا الجهاز (جهاز التوجيه) أو إرسال طلبات المصادقة إلى خادم خارجي مثل خادم ACS. لتحديد الطريقة التي سيتم استخدامها للمصادقة ، يتم استخدام قائمة طرق مصادقة افتراضية أو مخصصة.

٢- تفويض

يوفر إمكانات لفرض السياسات على موارد الشبكة بعد حصول المستخدم على حق الوصول إلى موارد الشبكة من خلال المصادقة. بعد نجاح المصادقة ، يمكن استخدام التفويض لتحديد الموارد التي يُسمح للمستخدم بالوصول إليها والعمليات التي يمكن إجراؤها.

على سبيل المثال ، إذا أراد مهندس شبكة مبتدئ (لا ينبغي له الوصول إلى جميع الموارد) الوصول إلى الجهاز ، فيمكن للمسؤول إنشاء طريقة عرض تسمح للمستخدم بتنفيذ أوامر معينة فقط (الأوامر المسموح بها في الطريقة قائمة). يمكن للمسؤول استخدام قائمة طرق التفويض لتحديد كيفية تفويض المستخدم لموارد الشبكة ، أي من خلال قاعدة بيانات محلية أو خادم ACS.

٣- محاسبة

يوفر وسيلة لمراقبة الأحداث التي يقوم بها المستخدم أثناء الوصول إلى موارد الشبكة والتقاطها. حتى أنه يراقب طول مدة وصول المستخدم إلى الشبكة.
يمكن للمسؤول إنشاء قائمة طريقة محاسبة لتحديد ما يجب محاسبته ولمن يجب إرسال السجلات المحاسبية.

تنفيذ AAA:

يمكن تنفيذ AAA باستخدام قاعدة البيانات المحلية للجهاز أو باستخدام خادم ACS خارجي.

قاعدة البيانات المحلية - إذا أردنا استخدام تكوين التشغيل المحلي لجهاز التوجيه أو التبديل لتنفيذ AAA ، فيجب علينا إنشاء المستخدمين أولاً للمصادقة وتوفير مستويات الامتياز للمستخدمين للمصادقة.

خادم ACS - هذه هي الطريقة الشائعة المستخدمة. يتم استخدام خادم ACS خارجي (يمكن أن يكون جهاز ACS أو برنامج مثبت على VMware) لـ AAA حيث يلزم التكوين على كل من جهاز التوجيه وACS. يتضمن التكوين إنشاء مستخدم ، وقائمة طرق مخصصة منفصلة للمصادقة ، والتفويض ، والمحاسبة.
يرسل العميل أو خادم الوصول إلى الشبكة (NAS) طلبات المصادقة إلى خادم ACS ويتخذ الخادم قرارًا للسماح للمستخدم بالوصول إلى مورد الشبكة أو ليس وفقًا لبيانات الاعتماد المقدمة من المستخدم.

ملاحظة - إذا فشل خادم ACS في المصادقة ، يجب أن يذكر المسؤول استخدام قاعدة البيانات المحلية للجهاز كنسخة احتياطية ، في قائمة الطرق لتنفيذ AAA.

بروتوكول التكوين الديناميكي للمضيف (DHCP)

هو بروتوكول إدارة شبكة يُستخدم على شبكات بروتوكول الإنترنت (IP) للتعيين التلقائي لعناوين IP ومعلمات الاتصال الأخرى للأجهزة المتصلة بالشبكة باستخدام بنية الخادم والعميل.

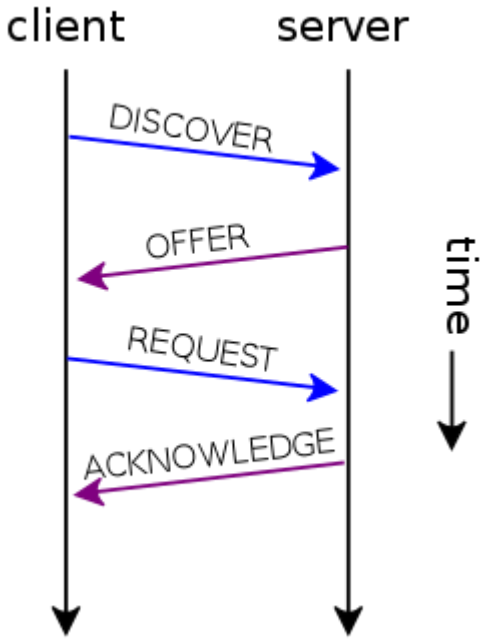
تلغي هذه التقنية الحاجة إلى تكوين أجهزة الشبكة يدويًا بشكل فردي ، وتتكون من مكونين للشبكة ، وخادم DHCP للشبكة مثبت مركزيًا ومثيلات العميل لمكدس البروتوكولات على كل كمبيوتر أو جهاز. عند الاتصال بالشبكة ، وبشكل دوري بعد ذلك ، يطلب العميل مجموعة من المعلمات من خادم DHCP باستخدام بروتوكول DHCP.

يمكن تنفيذ DHCP على شبكات تتراوح في الحجم من الشبكات السكنية إلى شبكات الحرم الجامعي الكبيرة وشبكات ISP الإقليمية. تحتوي العديد من أجهزة التوجيه والبوابات السكنية على إمكانية خادم DHCP. تتلقى معظم أجهزة توجيه الشبكة السكنية عنوان IP فريدًا داخل شبكة مزود خدمة الإنترنت. داخل الشبكة المحلية، يقوم خادم DHCP بتعيين عنوان IP محلي لكل جهاز.

تتواجد خدمات DHCP للشبكات التي تقوم بتشغيل الإصدار ٤ من بروتوكول الإنترنت (IPv4) ، بالإضافة إلى الإصدار ٦ (IPv6). يطلق على إصدار IPv6 من بروتوكول DHCP اسم DHCPv6.

يستخدم DHCP نموذج خدمة بدون اتصال ، باستخدام بروتوكول مخطط بيانات المستخدم (UDP). يتم تنفيذه برقمي منفذي UDP لعملياته وهما نفس رقم بروتوكول التمهيد (BOOTP). رقم منفذ UDP رقم ٦٧ هو المنفذ الوجهة للخادم ، ويستخدم العميل رقم منفذ UDP رقم ٦٨.

تنقسم عمليات DHCP إلى أربع مراحل: اكتشاف الخادم وعرض تأجير IP وطلب تأجير IP وإقرار تأجير IP. غالبًا ما يتم اختصار هذه المراحل باسم DORA للاكتشاف والعرض والطلب والاعتراف.



تبدأ عملية DHCP ببث العملاء للطلب. إذا كان العميل والخادم في نطاقات بث مختلفة ، فيمكن استخدام مساعد DHCP أو وكيل ترحيل DHCP. يمكن للعملاء الذين يطلبون تجديد عقد إيجار حالي an existing lease التواصل مباشرة عبر UDP أحادي الإرسال ، نظرًا لأن العميل لديه بالفعل عنوان IP محدد في تلك المرحلة.

بالإضافة إلى ذلك ، هناك علامة بث (١ بت في حقل إشارات ٢ بايت ، حيث يتم حجز جميع وحدات البت الأخرى وبالتالي يتم تعيينها على ٠) يمكن للعميل استخدامها للإشارة إلى الطريقة (البث أو البث الأحادي) التي يمكن أن يستقبل بها DHCPOFFER: 0x8000 للبث ، ٠x0000 للبث الأحادي. عادة ، يتم إرسال DHCPOFFER من خلال إرسال أحادي. بالنسبة لأولئك المضيفين الذين لا يمكنهم قبول حزم أحادية الإرسال قبل تكوين عناوين IP ، يمكن استخدام هذه العلامة للتغلب على هذه المشكلة.

يحدد بروتوكول الإنترنت (IP) كيفية اتصال الأجهزة داخل وعبر الشبكات المحلية على الإنترنت. يمكن لخادم DHCP إدارة إعدادات IP للأجهزة الموجودة على شبكته المحلية ، على سبيل المثال ، عن طريق تعيين عناوين IP لتلك الأجهزة تلقائيًا وديناميكيًا.

يعمل DHCP على أساس نموذج الخادم والعميل. عندما يتصل جهاز كمبيوتر أو جهاز آخر بشبكة ، يرسل برنامج عميل DHCP استعلام بث DHCP يطلب المعلومات الضرورية. يجوز لأي خادم DHCP على الشبكة خدمة الطلب. يدير خادم DHCP مجموعة من عناوين IP ومعلومات حول معلمات تكوين العميل مثل البوابة الافتراضية واسم المجال وخوادم الأسماء وخوادم الوقت. عند تلقي طلب DHCP ، قد يستجيب خادم DHCP بمعلومات محددة لكل عميل ، على النحو الذي تم تكوينه مسبقًا من قبل المسؤول ، أو بعنوان محدد وأي معلومات أخرى صالحة للشبكة بأكملها وللفترة الزمنية التي يتم فيها التخصيص (الإيجار) صالح. يستعلم عميل DHCP عادةً عن هذه المعلومات فور بدء التشغيل ، وبشكل دوري بعد ذلك قبل انتهاء صلاحية المعلومات. عندما يقوم عميل DHCP بتحديث مهمة ، فإنه يطلب في البداية نفس قيم المعلمات ، ولكن قد يقوم خادم DHCP بتعيين عنوان جديد بناءً على سياسات التعيين التي حددها المسؤولون.

على الشبكات الكبيرة التي تتكون من روابط متعددة ، قد يقوم خادم DHCP منفرد بخدمة الشبكة بأكملها عند الاستعانة بوكلاء ترحيل DHCP الموجودين على أجهزة التوجيه المتصلة. يقوم هؤلاء العملاء بترحيل الرسائل بين عملاء DHCP وخوادم DHCP الموجودة على شبكات فرعية مختلفة.

اعتمادًا على التنفيذ، قد يكون لخادم DHCP ثلاث طرق لتخصيص عناوين IP:

- التخصيص الديناميكي
يحتفظ مسؤول الشبكة بمجموعة من عناوين IP لـ DHCP ، ويتم تكوين كل عميل DHCP على الشبكة المحلية لطلب عنوان IP من خادم DHCP أثناء تهيئة الشبكة. تستخدم عملية الطلب والمنح مفهوم الإيجار بفترة زمنية يمكن التحكم فيها ، مما يسمح لخادم DHCP باستعادة عناوين IP التي لم يتم تجديدها ثم إعادة تخصيصها.
- التخصيص التلقائي
يقوم خادم DHCP بشكل دائم بتعيين عنوان IP للعميل الطالب من نطاق محدد من قبل المسؤول. هذا يشبه التخصيص الديناميكي ، لكن خادم DHCP يحتفظ بجدول لتعيينات عناوين IP السابقة ، بحيث يمكنه تعيين عنوان IP نفسه للعميل بشكل تفضيلي.
- التخصيص اليدوي
تسمى هذه الطريقة أيضًا بشكل مختلف تخصيص DHCP الثابت ، وتخصيص العنوان الثابت ، والحجز ، وربط عنوان IP / MAC. يقوم المسؤول بتعيين معرف فريد (معرف العميل أو عنوان MAC) لكل عميل إلى عنوان IP ، والذي يتم تقديمه للعميل الطالب. قد يتم تكوين خوادم DHCP للرجوع إلى طرق أخرى إذا فشل ذلك.
تُستخدم خدمات DHCP مع الإصدار ٤ من بروتوكول الإنترنت (IPv4) و IPv6. تختلف تفاصيل بروتوكول IPv4 و IPv6 بشكل كافٍ بحيث يمكن اعتبارهما بروتوكولات منفصلة. بالنسبة لعملية IPv6 ، قد تستخدم الأجهزة

بدلاً من ذلك التكوين التلقائي للعنوان عديم الحالة. قد يستخدم مضيفو IPv6 أيضًا عنونة الارتباط المحلي لتحقيق عمليات مقيدة بارتباط الشبكة المحلية.

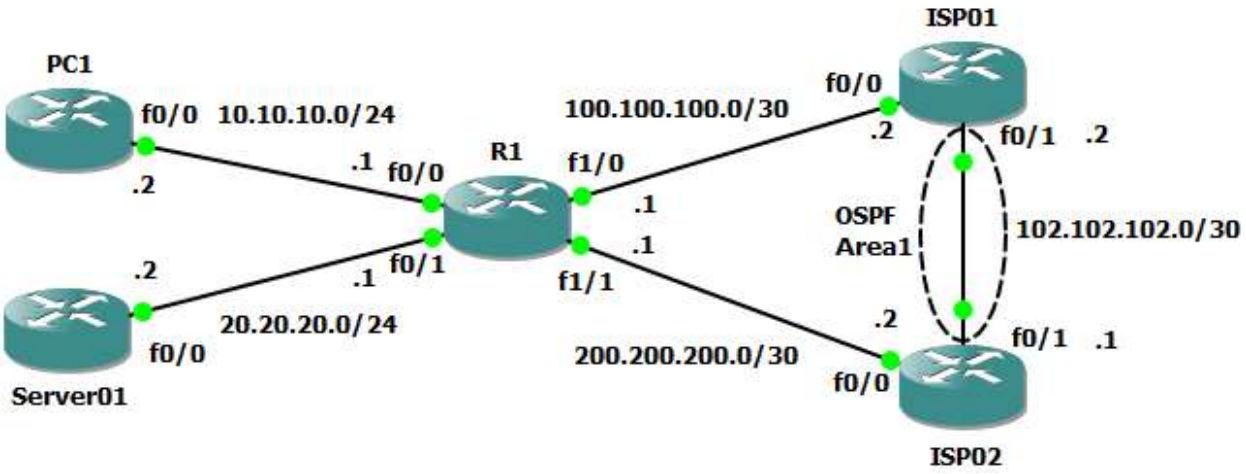
تكوين موازنة تحميل ISP المزدوج على روتر Cisco واحد

Configuring Dual ISP load balancing on Single Cisco Router

في الوقت الحالي ، ستحتاج الشبكة التي تحتوي على اتصالات إنترنت متعددة إلى موازن تحميل شبكة لتحميل الشبكات الفرعية. تعتبر موازنة التحميل مهمة جدًا ليس فقط في شبكات المؤسسات ولكن حتى في بعض الشبكات الصغيرة.

في معظم الحالات ، يريد الأشخاص أن يتمكن المستخدم النهائي من الوصول إلى الإنترنت باستخدام أكثر من مزود خدمة إنترنت لتحقيق هدف موازنة التحميل.

لتوضيح كيفية تكوين موازنة تحميل WAN مزدوجة على موجه Cisco واحد ، سنقوم بإعداد المخطط التالي:



هناك خمسة أجهزة توجيه ، الأول هو الموجه في شبكة الجامعة وسيعمل جهازي التوجيه الآخران كمزودي خدمة إنترنت مختلفين ، لذلك لدينا اتصالات إنترنت متعددة للشبكة الداخلية.

يستخدم مزود الخدمة الأول لخدمة اتصال الإنترنت لجهاز كمبيوتر المستخدم النهائي وهو ٢٤/١٠,١٠,١٠,٠ ويستخدم مزود الخدمة الثانى لخدمة اتصال الإنترنت للخوادم وهو ٢٤/٢٠,٢٠,٢٠,٠.

يوجد جهاز توجيه واحد PC1 داخل شبكة LAN يعمل كعميل كمبيوتر للمستخدم النهائي ويعمل جهاز توجيه واحد Server01 كخادم مخصص في منطقة الخوادم.

وبسبب محدودية الأوامر المتاحة على أجهزة الموجهات المستخدمة فى برنامج الباكت تريسر Packet Tracer فإن اللاب التالى لايمكن أن يتم عمله على برنامج الباكت تريسر حيث أنه لا يستخدم ال IOS IMAGE الحقيقى للروتر و لكنه محاكى فقط للأجهزة ، على عكس برنامج EVE-NG أو GNS3 اللذان يستخدمان ال IOS IMAGE الحقيقي كما لوكنت تعمل على جهاز روتر حقيقى به جميع الأوامر.

الآن دعنا نقوم بتكوين إعداد عنوان IP على PC1.

```
# int f0/0
    ip add 10.10.10.2 255.255.255.0
    no sh
# ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

في Server01 ، إعداد عنوان IP على النحو التالي:

```
# int f0/0
     ip add 20.20.20.2 255.255.255.0
     no sh
# ip route 0.0.0.0 0.0.0.0 20.20.20.1
```

على جهاز توجيه العميلR1 ، قم بتكوين إعدادات عنوان IP التالية

```
# int f0/0
      ip add 10.10.10.1 255.255.255.0
      no sh
# int f0/1
     ip add 20.20.20.1 255.255.255.0
     no sh
# int f1/0
     ip add 100.100.100.1 255.255.255.252
     no sh
# int f1/1
    ip add 200.200.200.1 255.255.255.252
    no sh
```

على جهاز التوجيه ISP01 ، قم بتكوين إعدادات عنوان IP التالية

```
# int f0/0
    ip add 100.100.100.2 255.255.255.252
    no sh
# int f0/1
    ip add 102.102.102.1 255.255.255.252
    no sh
```

على جهاز التوجيه ISP02 ، قم بتكوين إعدادات عنوان IP التالية

```
# int f0/0
    ip add 200.200.200.2 255.255.255.252
    no sh
# int f0/1
    ip add 102.102.102.2 255.255.255.252
    no sh
```

لتوصيل ISP01 بـ ISP02 ، نحتاج إلى تكوين بروتوكول توجيه. يمكن أن يكون بروتوكول التوجيه الثابت أو بروتوكول التوجيه الديناميكي ، ولكن في حالتنا الآن ، دعنا نستخدم بروتوكول التوجيه الديناميكي OSPF لتوصيل هذين ISP.

على جهاز التوجيه ISP01 ، قم بتكوين بروتوكول التوجيه الديناميكي OSPF على النحو التالي.

```
# router ospf 1
    net 102.102.102.0 0.0.0.3 area 1
    net 100.100.100.0 0.0.0.3 area 1
```

على جهاز التوجيه ISP02 ، قم بتكوين بروتوكول التوجيه الديناميكي OSPF على النحو التالي.

```
# router ospf 1
    net 102.102.102.0 0.0.0.3 area 1
    net 200.200.200.0 0.0.0.3 area 1
```

أول شيء يتعين علينا القيام به هنا للحصول على موازنة تحميل الإنترنت مع اتصالات الإنترنت المتعددة هو تكوين ترجمة عنوان الشبكة الديناميكية على جهاز توجيه Cisco R1 المتصل مباشرة بمزودي خدمة إنترنت.

لذلك ، يمكن لأجهزة الكمبيوتر العميلة في شبكة LAN الخاصة بالمستخدم والخوادم في مجموعة الخوادم LAN داخل الشبكة الداخلية الوصول إلى الإنترنت.

لتكوين NAT الديناميكي على جهاز توجيه Cisco R1 ، نحتاج إلى إنشاء قائمة تحكم في الوصول (ACL) لاحتواء عنوان IP الذي سيتم ترجمة عنوان URL إليه. في قائمة ACL أدناه ، نسمح لكل IP في أجهزة الكمبيوتر العميلة في شبكة LAN للمستخدم والخوادم في مزرعة الخوادم يمكن لشبكة LAN الوصول إلى الإنترنت.

```
# ip access-list standard ACL-UserLAN
     permit 10.10.10.0 0.0.0.255
# ip access-list standard ACL-ServerLAN
 permit 20.20.20.0 0.0.0.25
```

بعد تكوين قائمة التحكم في الوصول ، نحتاج إلى تكوين NAT الديناميكي باستخدام ACL الذي تم إنشاؤه أعلاه.

```
# int f0/0
    ip nat inside
# int f0/1
    ip nat inside
# int f1/0
    ip nat outside
# int f1/1
    ip nat outside
# ip nat inside source list ACL-ServerLAN int fa1/1 overload
# ip nat inside source list ACL-UserLAN int fa1/0 overload
```

بعد ذلك ، نحتاج إلى تكوين المسارات الافتراضية على جهاز توجيه Cisco R1 ذي الاتصال بالشبكة المزدوجة. لذلك ، يمكن لأجهزة كمبيوتر المستخدم النهائي في شبكة LAN الخاصة بالمستخدم والخوادم في مجموعة الخوادم LAN داخل الشبكة الداخلية الوصول إلى الإنترنت.

```
# ip route 0.0.0.0 0.0.0.0 100.100.100.2
# ip route 0.0.0.0 0.0.0.0 200.200.200.2
```

نحن الآن بحاجة إلى تكوين PBR للتوجيه المستند إلى السياسة على جهاز توجيه Cisco باستخدام اتصال مزدوج Wan R1. سيدير PBR التوجيه المستند إلى السياسة إعادة توجيه حركة المرور من كمبيوتر المستخدم النهائي LAN 10.10.10.0/24 إلى الإنترنت عبر ISP01 ومجموعة الخوادم LAN إلى الإنترنت عبر ISP02.

```
# route-map PBR-UserLAN permit 10
    set ip next-hop 100.100.100.2
    match ip address ACL-UserLAN
# route-map PBR-SERVERLAN permit 10
    set ip next-hop 200.200.200.2
    match ip address ACL-ServerLAN
```

بعد ذلك ، نحتاج إلى تطبيق PBR للتوجيه المستند إلى السياسة والذي تم تكوينه أعلاه في الواجهة المتصلة بشبكة LAN للمستخدم النهائي ومزرعة الخوادم LAN.

```
# int f0/0
      ip policy route-map PBR-UserLAN
# int f0/1
     ip policy route-map PBR-SERVERLAN
```

لاختبار ما إذا كان تكوين موازنة تحميل ISP مع اتصالات الإنترنت المتعددة يعمل أم لا ، يمكننا اختبار الاتصال على عنوان IP العام لهذين ISP وهو ١٠٢,١٠٢,١٠٢,١ أو ١٠٢,١٠٢,١٠٢,٢ من كمبيوتر المستخدم النهائي LAN PC1 أو Server01 في شبكة الخوادم LAN. يجب أن نحصل على النتيجة الناجحة التالية.

```
PC1# ping 102.102.102.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.102.102.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/50/72 ms

Server01# ping 102.102.102.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.102.102.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/48 ms
```

بعد أن علمنا أن الأمر ping لعنوان IP العام لمزودي خدمة الإنترنت هذين ناجح ، يمكننا التحقق من الأمر traceroute لمعرفة المسار الذي سيصل إليه للوصول إلى عنوان IP العام. استنادًا إلى نتيجة التتبع التالية ، تصل إلى ١٠٢,١٠٢,١٠٢,٢ عبر ISP01.

```
PC1# traceroute 102.102.102.2

 1 10.10.10.1 36 msec 16 msec 8 msec
 2 100.100.100.2 8 msec 28 msec 16 msec
 3 102.102.102.2 52 msec 40 msec 44 msec

Server01# traceroute 102.102.102.1
 1 20.20.20.1 28 msec 20 msec 20 msec
 2 200.200.200.2 8 msec 36 msec 20 msec
 3 102.102.102.1 28 msec 36 msec 64 msec
```

استنادًا إلى نتيجة traceroute التالية ، يمكننا أن نرى أن كمبيوتر المستخدم النهائي PC1 يمكن أن يصل إلى ١٠٢,١٠٢,١٠٢,٢ عبر ISP01 ويمكن أن يصل Server01 في مزرعة الخوادم إلى ١٠٢,١٠٢,١٠٢,١ عبر ISP02.

اسمح أيضًا بالتحقق من تكوين NAT لموازنة تحميل ISP مع عمل اتصالات الإنترنت المتعددة أم لا. بالنسبة إلى شبكة LAN 10.10.10.0/24 للمستخدم النهائي ، يجب أن تتم ترجمة عنوان IP الخاص بـ ISP01 إلى عنوان IP الخاص بـ ISP01 ولمزرعة الخوادم ، يجب ترجمة شبكة LAN 20.20.20.0/24 إلى عنوان IP الخاص بـ ISP02 على النحو التالي.

```
# sh ip nat translations
Pro Inside global Inside local Outside local Outside global
udp 100.100.100.1:49323 10.10.10.2:49323 102.102.102.2:33437
102.102.102.2:33437
udp 100.100.100.1:49327 10.10.10.2:49327 102.102.102.2:33441
102.102.102.2:33441
udp 100.100.100.1:49328 10.10.10.2:49328 102.102.102.2:33442
102.102.102.2:33442
udp 200.200.200.1:49264 20.20.20.2:49264 102.102.102.1:33437
102.102.102.1:33437
udp 200.200.200.1:49265 20.20.20.2:49265 102.102.102.1:33438
102.102.102.1:33438
udp 200.200.200.1:49266 20.20.20.2:49266 102.102.102.1:33439
102.102.102.1:33439
```

هذا كل شيء عن كيفية تكوين موازنة تحميل ISP المزدوجة على جهاز توجيه Cisco واحد . هذه طريقة رخيصة وبسيطة لتحقيق هدف موازنة حمل مزود خدمة الإنترنت مع اتصالات الإنترنت المتعددة.

- المراجع
  - Implementing Cisco Network Security (IINS)
  - ccnp security core scor 300-701 official cert guide
  - https://www.packetlife.net
  - https://www.flackbox.com/
  - https://www.udemy.com
  - https://www.itprotv.com

الخاتمة

وفي ختام هذا البحث وبعد أن بذلنا كل جهدنا وطاقتنا من أجل إخراجه على هذا الوجه؛ نحمد الله تعالى على هذا العمل، ونأمل أن يكون بمثابة الدليل الذي يضع كل باحث على النهج الصحيح الخاص بشبكات المعلومات والسرية وعلى الرغم من الجهد المبذول في هذا البحث؛ إلا أن هدفنا الأساسي في توضيح العديد من النقاط الغامضة كان هو المحفز لنا طوال الوقت من أجل تقديم عمل مُفيد ونافع، ونعتذر عن أي تقصير نكون قد وقعنا به دون قصد.