جامعة حماة
الكلية التطبيقية
قسم تقنيات حاسوب
السنة الرابعة
إدارة شبكات /٢/

المحاضرة الربعة

الوصول عن بعد وحماية الوصول إلى الشبكة

إعداد : م . إناس عدي

remote access server

ماهو remote access server :

هو عبارة عن جهاز (سيرفر) ننصب عليها خدمة remote access serves

من وظائفه :

١- معالجة المستخدمين الذين ليسو على الشبكة LAN وبحاجة للصول لها عن بعد والاستفادة من الموارد الموجودة عليها .

٢- يقوم ببناء tunnel (vpn) بينه وبين ال client حيث تقوم بتشفير البيانات المرسلة من ال client إلى RAS .

وذلك لان طريقة الاتصال بين ال client وال RAS تتم عن طريق شبكة الانترنيت وهي PUBLIC وبالتالي معرضة للتهكير .

لذلك عند استخدام ال RAS يقوم ببناء ال Tunnel لحل هذه المشكلة .

طريقة عمل remote access server

عندما يقوم ال client بالاتصال بالشبكة عن بعد يمر بثلاث مراحل :

- Identification : حيث يقوم بإرسال اسم المستخدم للسيرفر ، ويقوم السيرفر عند استقبالها بالتحقق منها .
- Authentication : يقوم المستخدم بإرسال كلمة المرور وأيضا يقوم السيرفر بالتحقق من ذلك .

- Authorization : وهي الخدمات التي يمكن للمستخدم ان يقوم بها .

وتكون بثلاث حالات :

- ✓ deny : غير متاح له بالدخول
- ✓ allow : متاح له بالدخول واستخدام أي شي من الموارد
- ✓ control throw policy : أي حتى بعد التحقق من هذا ال client لا يسمح له بالدخول إلا إذا حقق الشروط المطبقة عليه من خلال (NPS) .

ملاحظة : RAS له كرتين شبكة احدهما Internal للاتصال بالشبكة المحلية والأخر External للاتصال بشبكة الانترنيت .

Network Access Protection

(NAP)

ما هو ال NAP :

- هو عبارة عن تقنية صممتها مايكروسوفت للحفاظ على أجهزة المستخدمين والسيرفرات من الأجهزة التي تحاول الولوج إلى الشبكة الداخلية للشركة كأجهزة الزبائن وأصدقاء الشركة أو المستخدمين الذين يستعملون حواسيب محمولة خارج الشركة وداخلها .وليس لديهم حماية ضد الفيروسات والملفات الخبيثة أو أن برنامج الحماية وأنظمة التشغيل لديهم غير محدثة بأخر التحديثات مما يسهل عملية إصابتها بالفيروسات لذلك فهي تشكل خطرا على الشبكة الداخلية للشركة ولهذا يقوم بجمع وإدارة المعلومات الصحية لكل عنصر على الشبكة .

- يستخدم NAP لتعقيم صحة الكمبيوتر (client) الذي يأتي مقارنة بالسياسات الموضوعة في الشبكة ، والتي توضع (NAP).

- إذا كان الجهاز غير مطابق لكل المتطلبات الموضوعة من إدارة الشبكة سوف يتم إرساله إلى (Remediation Network) لحل المشكلة التي تواجه الجهاز.

NAP Enforcement type : طرق النفاذ والوصول إلى الشبكة والتي نطبق NAP عليها :

١- إنفاذ nap باستخدام dhcp :

يمكن فرض السياسات الصحية napعندما يحاول العميل الحصول على عنوان ip أو تجديده من dhcp لا يستطيع إذا لم تكن بياناته الصحية موافقة للبيانات الموضوعة وبالتالي لا يستطيع الاتصال بالشبكة إلا بعد فرض البيانات الصحية على العميل ولكن هو أسلوب الأقل أمان حيث يمكن للمستخدم تكوين يدويا عنوان ip على جهاز وتجاوز تنفيذ سياسة NAP DHCP

٢- إنفاذ nap باستخدام مخدمات vpn:

وبهذه الطريقة سوف نستخدم (NPS) في عمليات الاتصال وتحقق في العملية وتنفيذ السياسات الصحية وذلك عندما يحاول العميل الاتصال بالشبكة من خلال اتصال VPN وهو خيار إنفاذ خطة NAP للاهتمام بالعملاء البعدين عن جانب الملقم والأسلوب الوحيد الذي يتطلب إنفاذ اثنين من العملاء مع تمكين الاتصال من جانب العميل حيث يقوم بإعطاء IP. لأجهزة التي تدخل إلى الشبكة وضعها بما يسمى الحجر الصحي ليتم تنفيذ السياسات الصحية قبل السماح لها بالاتصال .

٣- إنفاذ NAPبالاستخدام 802.1X

عندما يقوم المستخدم بالاتصال بالشبكة باستخدام نقاط الوصول اللاسلكية يقوم NAPبوضع الأجهزة الغير المتوافقة على شبكة خاصة للمعالجة ويتم تقيدها للوصول للشبكة الأساسية من خلال تطبيق مرشحات IP

٤- إنفاذ ال NAP باستخدام IPSec

تتألف ال NAP من اثنين من الخدمات :

System heath agent (SHA) :

وهو الذي يقوم بتقديم الحالة الصحية له ويرسله الى (SHV) .

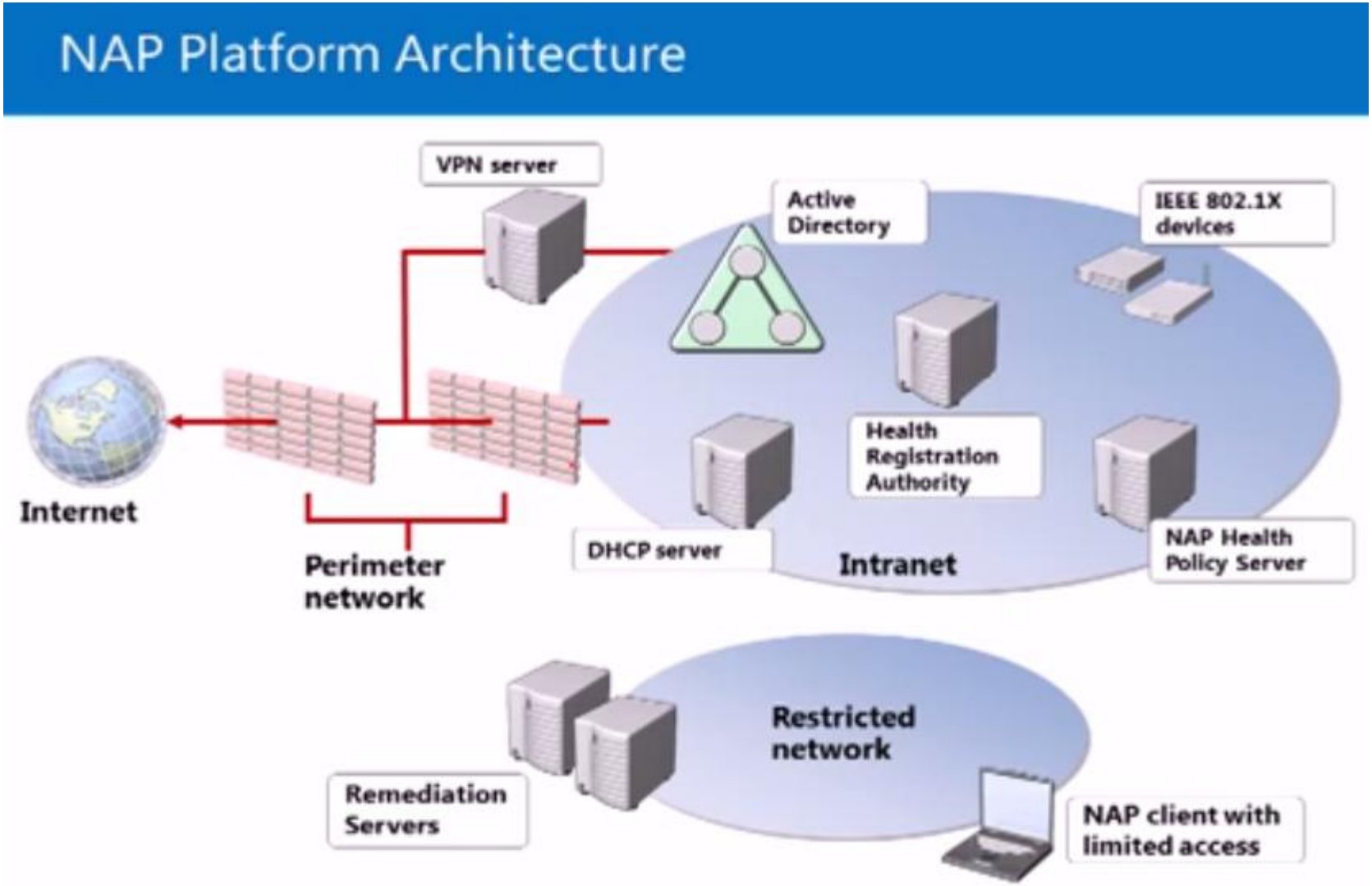
System health validation (SHV):

السيرفر يحلل المعلومات المقدمة من (SHA) إذا كانت متوافقة يمكن لها بالدخول إلى الشبكة ،أما إذا كانت غير متوافقة يتم وضعه في (Remediation) ليتم معالجته .

ملاحظة :

Network Policy Server (NPS):وهي التي يتم من خلالها وضع POLICY(سياسة) التي يمكن تطبيقها وفرضها على المستخدمين وذلك لحماية الوصول إلى الشبكة

طريقة عمل NAP



طريقة عمل NAP

عندما يقوم Client بالاتصال بالشبكة عبر نقاط النفاذ التي تم ذكرها سابقا مثلا عن طريق dhcp

١- يقوم ال client بتقديم الحالة الصحية له (SHA) إلى (SHV)

٢- (SHV) يقوم بالتحقق فيما إذا كانت الحالة الصحية (SOF) ل clientموافقة للسياسات الموضوعة من قبل الشركة ، إذا كانت موافقة لهذه السياسات يتم السماح له بالدخول إلى الشبكة

٣- إذا لم يكن محقق لكل السياسات الموضوعة من قبل إدارة الشبكة يتم تحويله إلى Restricted Network أي يتم عزله عن الشبكة الحقيقة ريثما يتم تعقيم له (معالجته) وذلك عن طريق (Remediation Network)

٤- وبعد ما يتم معالجة مشكلة client يسمح له بالدخول إلى الشبكة .

ما هي شبكة VPN

هي اختصار ل Virtual Private Network وتعني الشبكة الخاصة الظاهرية
وهي عبارة عن توصيل جهازين أو شبكتين معا عن طريق شبكة الانترنت كما هو موضح في الصورة
وهي تقنية تعتمد في عملها على بروتوكول حيث يطلق عادة على عملية انشاء اتصال خاص بين جهازي كمبيوتر من خلال شبكة وسيطة كالانترنت اسم نقل البيانات عبر مسار امن (Tunneling)
حيث يتم إنشاء هذا المسار بين جهازي الكمبيوتر مباشرة.

ما هي البروتوكولات المعتمدة عليها تقنية VPN :

PPTP : Point-To-Point Tunneling Protocol

L2TP : Layer Two Tunneling Protocol

مميزات وعيوب استخدام VPN :

المميزات:

١- يوفر الكثير من المال خاصة في تكاليف الأجهزة.

٢- يسهل ادارتة

عيوبه:

- إذا لم تقوم بتوثيق المستخدمين والشبكات بشكل قاطع ستصبح هناك فرصة للمتطفلين للوصول إلى بياناتك

The End