Groupe de travail Réseau
Request for Comments : 5209
Catégorie : Information
Traduction Claude Brière de L'Isle

P. Sangster, Symantec
H. Khosravi, Intel
M. Mani, Avaya
K. Narayan, Cisco Systems
J. Tardo, Nevis Networks
juin 2008

Évaluation de point d'extrémité de réseau (NEA) : généralités et exigences

Statut du présent mémoire

Le présent mémoire fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document définit le problème, la portée, et les exigences de protocole entre les composants du modèle de référence d'évaluation de point d'extrémité de réseau (NEA, *Network Endpoint Assessment*). NEA fournit aux propriétaires de réseaux (par exemple, une entreprise qui offre l'accès à distance) un mécanisme pour évaluer la posture d'un système. Cela peut avoir lieu durant la demande d'accès au réseau et/ou ensuite à tout moment pendant la connexion au réseau. Les informations de posture apprises peuvent alors être appliquées à diverses décisions en rapport avec la conformité. Les informations de posture sont fréquemment utiles pour détecter les systèmes qui manquent ou ont des mécanismes de protection de la sécurité dépassés comme des anti-virus et un logiciel de pare-feu fondé sur l'hôte. Afin de fournir un contexte pour les exigences, on introduit un modèle de référence et une terminologie.

Table des Matières

1. Introduction

Les points d'extrémité connectés à un réseau peuvent être exposés à une large variété de menaces. Une certaine protection contre ces menaces peut être fournie en s'assurant que les points d'extrémité se conforment aux politiques de sécurité. Donc, l'intention de NEA est d'assurer que ces points d'extrémité déterminent leur conformité aux politiques de sécurité afin que des mesures correctives puissent être fournies avant qu'ils soient exposés à ces menaces. Par exemple, si il est déterminé qu'un système n'est pas conforme parce qu'il manque des mécanismes de défense appropriés comme des pare-feu fondés sur l'hôte, un logiciel anti-virus, ou à cause de l'absence de correctifs de sécurité critiques, les protocoles NEA fournissent un mécanisme pour détecter ce fait et indiquer les actions correctives appropriées à prendre. Noter qu'un point d'extrémité qui est réputé conforme peut quand même être vulnérable à des menaces qui peuvent exister sur le réseau.

NEA implique normalement l'utilisation d'un logiciel client spécial fonctionnant sur le point d'extrémité demandeur, qui observe et rapporte la configuration du système à l'infrastructure du réseau. L'infrastructure a un logiciel de validation correspondant qui est capable de comparer les informations de configuration du point d'extrémité aux politiques de conformité du réseau et de fournir le résultat aux entités d'autorisation appropriées qui prennent les décisions sur l'accès au réseau et aux applications. Certains points d'extrémité peuvent être incapables de faire fonctionner le logiciel de client NEA (par exemple, une imprimante) ou ne pas vouloir partager les informations sur leur configuration. Cette situation sort du domaine d'application de NEA et est soumise aux politiques locales.

Le résultat de l'évaluation d'un point d'extrémité peut influencer une décision d'accès provisionnée aux mécanismes d'application sur le réseau et/ou au point d'extrémité qui demande l'accès. Bien que le groupe de travail NEA reconnaisse qu'il peut y avoir un lien entre une évaluation et l'application d'une décision d'accès résultante, les mécanismes et protocoles pour l'application sortent du domaine d'application de cette spécification.

Des architectures, similaires à NEA, ont existé dans l'industrie depuis un certain temps et sont présentes dans des produits du commerce, mais n'offrent pas une interopérabilité adéquate. Des exemples de telles architectures incluent la connexion de réseau de confiance (TNC, *Trusted Network Connect)* [TNC] du groupe "Trusted Computing", la protection d'accès réseau (NAP, *Network Access Protection*) [NAP] de Microsoft, et le contrôle d'admission réseau Cisco (CNAC, *Cisco Network Admission Control*) [CNAC]. Ces technologies évaluent le logiciel et/ou la configuration matérielle des appareils de point d'extrémité pour les besoins de surveillance ou d'application de la conformité à la politique d'une organisation.

Le groupe de travail NEA développe des protocoles standard qui peuvent être utilisés pour communiquer des informations de conformité entre un client et un serveur NEA. Le présent document donne le contexte pour NEA incluant la terminologie, l'applicabilité, la déclaration de problème, le modèle de référence, et les cas d'utilisation. Il identifie ensuite les exigences pour les protocoles utilisés pour communiquer entre un client et un serveur NEA. Finalement, le présent document discute des considérations potentielles de sécurité et de confidentialité de l'utilisation de NEA. La plus grande partie de cette spécification est constituée de texte pour information qui décrit le contexte de NEA.

1.1 Langage des exigences

L'utilisation de mots en majuscules dans une phrase a la signification suivante dans le processus de choix de protocole du groupe de travail NEA :
DOIT – indique une exigence absolue.
NE DOIT PAS – indique quelque chose d'absolument interdit.
DEVRAIT – indique une forte recommandation d'un résultat désiré.
NE DEVRAIT PAS – indique une forte recommandation contre un résultat.
PEUT – indique la volonté de permettre un résultat facultatif.

L'utilisation des mots "doit", "ne doit pas", "devrait", "ne devrait pas", et "peut" en minuscules a sa signification normale et n'est pas soumise à ces définitions.

2. Terminologie

Cette section définit un ensemble de termes utilisés dans le présent document. Dans certains cas, ces termes ont été utilisés dans d'autres contextes avec une signification différente de sorte que cette section tente de décrire la signification de chaque terme par rapport aux activités du groupe de travail NEA.

Évaluation : processus de collecte de posture pour un ensemble de capacités sur le point d'extrémité (par exemple, pare-feu fondé sur l'hôte) de façon à ce que les valideurs appropriés puissent évaluer la posture par rapport à une politique de conformité.

Attributs d'évaluation : attributs qui incluent des informations réutilisables sur le succès d'une évaluation précédente du point d'extrémité. Cela pourrait être utilisé pour optimiser des évaluations suivantes en évitant une réévaluation complète de la posture. Par exemple, cette classification d'attribut pourrait être produite spécifiquement à un point d'extrémité particulier, datée et signée par le serveur NEA permettant à ce point d'extrémité de la réutiliser pendant un certain temps pour attester de la conformité à un ensemble de politiques. Le serveur NEA pourrait accepter cela au lieu d'obtenir les informations de posture.

Attribut : élément de données incluant toutes méta-données requises décrivant un état observé, attendu, ou opérationnel d'une caractéristique d'un point d'extrémité (par exemple, le logiciel anti-virus utilisé actuellement). Les attributs sont échangés au titre des protocoles NEA (voir le paragraphe 5.2). NEA reconnaît divers scénarios d'usage où l'utilisation d'un attribut dans un type particulier de message pourrait indiquer :
o l'état attesté précédemment (attributs d'assertion),
o la configuration ou propriété observée (attributs de posture),
o une demande d'informations de configuration ou de propriété (attributs de demande),
o une décision d'attestation (attributs de résultat) ou
o des instructions de réparation (attributs de remède).
Le groupe de travail NEA va normaliser un sous ensemble de l'espace de noms d'attributs connus comme attributs standard. Les attributs non standardisés sont appelés "spécifiques du fabricant" dans la présente spécification.

Dialogue : séquence de messages de demande/réponse échangés.

Point d'extrémité : tout appareil informatique qui peut être connecté à un réseau. De tels appareils sont normalement associés à une adresse de couche de liaison particulière avant de se joindre au réseau et potentiellement à une adresse IP une fois sur le réseau. Cela inclut des ordinateurs portables, tablettes, serveurs, téléphones cellulaires, ou tout appareil qui peut avoir une adresse IP.

Message : unité de communication auto contenue entre le client et le serveur NEA. Par exemple, un message d'attribut de posture pourrait porter un ensemble d'attributs décrivant la configuration du logiciel anti-virus sur un point d'extrémité.

Propriétaire : rôle d'une entité qui est le possesseur légal, de plein droit, d'un bien (par exemple, le point d'extrémité). Le propriétaire est en droit de maintenir le contrôle sur les politiques appliquées sur l'appareil même si le bien n'est pas en la possession du propriétaire. Le propriétaire peut permettre d'outrepasser l'utilisateur ou l'augmentation des politiques de contrôle ou peut choisir de ne pas affirmer de politique limitant l'utilisation du bien.

Posture : configuration et/ou état d'un matériel ou logiciel sur un point d'extrémité lorsque il relève de la politique de sécurité d'une organisation.

Attributs de posture : attributs qui décrivent la configuration ou l'état (posture) d'une caractéristique du point d'extrémité. Par exemple, un attribut de posture pourrait décrire la version du système d'exploitation installé sur le système.

Attributs de demande : attributs envoyés par un serveur NEA qui identifient les informations de posture demandées du client NEA. Par exemple, un attribut de demande pourrait être un attribut inclus dans un message de demande du serveur NEA qui veut avoir les informations de version du système d'exploitation sur le point d'extrémité.

Attributs de remède : attributs contenant les instructions de remède sur la façon de mettre un point d'extrémité en conformité avec une ou plusieurs politiques. Le groupe de travail NEA ne définit pas d'attributs de remède standard, mais cette spécification décrit où ils sont utilisés dans le modèle de référence et les protocoles.

Attributs de résultat : attributs qui décrivent si le point d'extrémité est conforme à la politique NEA. L'attribut de résultat est créé normalement par le serveur NEA à la conclusion de l'évaluation pour indiquer si le point d'extrémité a été considéré conforme ou non. Plus d'un de ces attributs peut être utilisé pour permettre que des décisions de niveau de caractéristique plus fin soient communiquées en plus d'une décision d'évaluation globale.

Session : une connexion à états pleins capable de porter plusieurs échanges de messages associés à une ou des évaluations d'un point d'extrémité particulier. Le présent document définit le terme de session à un niveau conceptuel et ne décrit pas les propriétés de la session ni ne spécifie les exigences pour que les protocoles NEA gèrent ces sessions.

Utilisateur : rôle d'une personne qui fait usage des services d'un point d'extrémité. L'utilisateur peut n'être pas le propriétaire du point d'extrémité dont il pourrait avoir besoin pour opérer dans les contraintes d'utilisation acceptables définies par le propriétaire du point d'extrémité. Par exemple, l'employé d'une entreprise pourrait être un utilisateur d'un ordinateur fourni par l'entreprise (propriétaire) pour les besoins du travail.

3. Applicabilité

Cette section discute de la portée des technologies qu'on normalise et des environnements de réseau où il est envisagé que les technologies de NEA pourraient être applicables.

3.1 Domaine d'application

La priorité du groupe de travail NEA est de développer des protocoles standard aux couches supérieures du modèle de référence (Section 5) : le protocole d'attribut de posture (PA, *Posture Attribute*) et protocole de courtier de posture (PB, *Posture Broker*). Un PA et un PB sont destinés à être portés sur divers protocoles de transport de couche inférieure (PT). Le groupe de travail NEA va identifier les protocoles PT standard de mise en œuvre obligatoire. Les protocoles PT peuvent être définis dans d'autres groupes de travail parce que les exigences peuvent n'être pas spécifiques de NEA. Quand ils sont utilisés avec un protocole PT standard (par exemple, le protocole d'authentification extensible (EAP) la sécurité de la couche transport (TLS) [RFC4346]) les protocoles de PA et PB vont permettre l'interopérabilité entre un client NEA d'un fabricant et un serveur NEA d'un autre fabricant. La présente spécification ne se concentre pas sur les autres interfaces entre les composants fonctionnels du modèle de référence NEA ni sur leurs exigences internes. Toute la discussion de ces aspects est incluse pour donner le contexte permettant de comprendre le modèle et les exigences qui en résultent.

Des zones tangentes non montrées dans le modèle de référence qui sortent aussi du domaine du groupe de travail NEA, et donc de la présente spécification, incluent :
- de normaliser les protocoles et mécanismes pour appliquer les restrictions d'accès au réseau ;
- de développer des protocoles standard pour remédier aux points d'extrémité non conformes ;
- de spécifier les protocoles utilisés pour communiquer avec les portions distantes des clients ou serveurs NEA (par exemple, des collecteurs ou valideurs distants de posture) ;
- de prendre en charge un client NEA qui fournit une posture pour d'autres points d'extrémité (par exemple, un client NEA sur un système de détection d'intrusion (IDS, *Intrusion Detection System*) fournissant la posture pour un point d'extrémité sans un client NEA) ;
- de définir l'ensemble d'événements ou situations qui pourraient déclencher la demande d'une attestation par un client NEA ou un serveur ;
- de détecter ou traiter les points d'extrémité menteurs (voir plus d'informations au paragraphe 8.1.1.

3.2 Applicabilité des environnements

Parce que le modèle NEA se fonde sur la présence d'un logiciel orienté NEA sur le point d'extrémité et dans l'infrastructure du réseau, et du fait de la nature des informations exposées, l'utilisation des technologies de NEA ne peut pas s'appliquer dans toutes les situations possibles sur l'Internet. Donc, cette section discute certains des scénarios où NEA a le plus de chances d'être applicable et de certains où il ne peut pas l'être. Finalement, l'utilisation de NEA dans un déploiement ne se restreint pas à ces seuls scénarios. La décision d'utiliser les technologies de NEA appartient à l'exploitant (par exemple, le fournisseur du réseau) sur la base des relations attendues qu'il a avec les propriétaires et les utilisateurs des points d'extrémité potentiels.

Les technologies de NEA sont largement concentrées sur des scénarios où le propriétaire du point d'extrémité est le même que celui du réseau. C'est un modèle très courant pour les entreprises qui fournissent des équipements à leurs employés pour effectuer leurs tâches. Ces employés sont probablement liés par un contrat de travail qui mentionne le niveau de visibilité que l'employeur attend de l'utilisation par les employés des biens de l'entreprise et des activités possibles pendant les heures de travail. Ce contrat peut établir l'attente que le point d'extrémité doive se conformer aux politiques établies par l'entreprise.

Certains autres environnements peuvent être dans une situation similaire et donc trouver bénéfiques les technologies de NEA. Par exemple, les environnements où le point d'extrémité est possédé par une partie (éventuellement l'utilisateur) qui a explicitement exprimé le désir de se conformer aux politiques établies par un fournisseur de réseau ou de services en échange d'être capable d'accéder à ses ressources. Un exemple en pourrait être un contractant indépendant avec un ordinateur portable, travaillant pour une entreprise qui impose les politiques d'évaluation de NEA à ses employés, qui peut

souhaiter un niveau similaire d'accès et qui veut se conformer à la politique de l'entreprise. Les technologies de NEA peuvent être applicables à cette situation.

À l'inverse, certains environnements où NEA n'est pas supposé être applicable seraient des environnements où le point d'extrémité est possédé par un utilisateur qui n'a pas accepté de se conformer à la politique d'un fournisseur de réseau. Un exemple pourrait inclure le cas où le contractant ci-dessus visite une zone publique comme le café du coin qui offre un accès Internet. On ne peut pas supposer que ce café soit capable d'utiliser les technologies de NEA pour évaluer la posture de l'ordinateur portable du contractant. À cause de la nature potentiellement invasive de la technologie de NEA, une telle évaluation pourrait s'apparenter à une invasion de la vie privée du contractant.

Il est plus difficile de déterminer si NEA est applicable dans d'autres environnements, de sorte que le groupe de travail NEA va les considérer comme sortant de son domaine de compétence et de spécification. Pour qu'un environnement soit considéré comme applicable pour NEA, le propriétaire ou l'utilisateur d'un point d'extrémité doit avoir établi une claire attente qu'il va se conformer aux politiques du propriétaire et de l'opérateur du réseau. Une telle attente inclut probablement la volonté de divulguer les informations appropriées nécessaires pour que le réseau effectue les vérifications de conformité.

4. Position du problème

La technologie NEA peut être utilisée pour divers objets. Cette section met en lumière certaines des situations majeures où les technologies de NEA peuvent être bénéfiques.

Une utilisation est de faciliter la vérification de la conformité d'un point d'extrémité à la politique de sécurité d'une organisation quand un point d'extrémité se connecte au réseau. Les organisations exigent souvent des points d'extrémité qu'ils fonctionnent avec une configuration de système d'exploitation (OS, *Operating System*) spécifiée par les technologies de l'information (IT, *Information Technologies*) et ait certaines applications de sécurité activées, par exemple, un logiciel anti-virus, des systèmes de détection/prévention d'intrusion de l'hôte, des pare-feu personnels, et un logiciel de gestion des réparations. Un point d'extrémité qui n'est pas conforme à la politique d'IT peut être vulnérable à un certain nombre de menaces connues qui pourraient exister sur le réseau.

Sans la technologie NEA, s'assurer de la conformité des points d'extrémité à la politique d'entreprise est une tâche difficile et fastidieuse. Tous les points d'extrémité ne sont pas gérés par une organisation de technologies de l'information d'une entreprise, par exemple, les laboratoires et les machines de contractants. Même pour les biens qui sont gérés, ils ne peuvent pas recevoir des mises à jour en temps utile parce qu'ils ne sont pas rattachés en permanence au réseau d'entreprise, par exemple, les portables. Avec la technologie NEA, le réseau est capable d'évaluer un point d'extrémité aussitôt qu'il demande l'accès au réseau ou à tout moment après qu'il s'est joint au réseau. Cela donne à l'entreprise une opportunité de vérifier la conformité de tous les points d'extrémité à capacité NEA en temps utile et facilite la correction du point d'extrémité éventuellement quand une quarantaine est nécessaire.

La technologie NEA peut être utilisée pour fournir l'évaluation de posture pour une gamme de façons de se connecter au réseau incluant (mais non limitée) l'accès aux LAN filaires et sans fil comme d'utiliser 802.1X [802.1X], l'accès à distance via IPsec [RFC4301], ou un VPN de couche de prise sécurisée (SSL, *Secure Socket Layer*) ou l'accès à une passerelle.

Les points de terminaison qui ne sont pas compatibles avec la NEA ou qui choisissent de ne pas partager une posture suffisante pour évaluer la conformité peuvent être soumis à des politiques d'accès différentes. La décision de gérer les points d'extrémité non conformes ou non participants peut être prise par l'administrateur du réseau, éventuellement sur la base d'informations provenant d'autres mécanismes de sécurité sur le réseau (par exemple, l'authentification). Par exemple, les instructions de remédiation ou les avertissements peuvent être envoyés à un point d'extrémité non conforme avec un utilisateur dûment autorisé tout en autorisant un accès limité au réseau. De plus, les technologies d'accès au réseau peuvent utiliser les résultats de la NEA pour restreindre ou refuser l'accès à un point d'extrémité, tout en permettant de corriger les vulnérabilités avant qu'un point d'extrémité ne soit exposé à une attaque. La communication et la représentation des résultats de l'évaluation de la NEA aux technologies d'accès au réseau sur le réseau sortent du domaine d'application de ce document.

La réévaluation est une deuxième utilisation importante de la technologie NEA, car elle permet d'effectuer des évaluations supplémentaires de points d'extrémité précédemment considérés comme conformes. Cela peut devenir nécessaire car les politiques de conformité du réseau et/ou posture de point d'extrémité peuvent changer au fil du temps. Un système initialement évalué comme étant conforme au moment de son intégration au réseau peut ne plus être en conformité après que des changements sont survenus. Par exemple, une réévaluation pourrait être nécessaire si un utilisateur désactive une protection de sécurité (par exemple, un pare-feu fondé sur l'hôte) exigée par la politique ou lorsque le pare-feu devient non conforme après qu'un correctif de pare-feu est émis et que la stratégie réseau est modifiée pour exiger le correctif.

Une troisième utilisation de la technologie NEA peut être de vérifier ou de compléter les informations sur les actifs de l'organisation mémorisées dans les bases de données d'inventaire.

La technologie NEA peut également être utilisée pour vérifier et rapporter la conformité des points d'extrémité lorsqu'ils tentent d'accéder à certaines applications critiques au sein d'une entreprise, en utilisant une évaluation déclenchée par le service (application).

5. Modèle de référence

Cette section décrit le modèle de référence pour l'évaluation des points de terminaison réseau. Ce modèle est fourni pour établir un contexte pour la discussion des exigences et ne peut pas être directement associé à un produit particulier ou à une architecture de déploiement. Le modèle identifie les fonctionnalités majeures du client et serveur NEA et leurs relations, ainsi que les protocoles qu'ils utilisent pour communiquer à différents niveaux (par exemple, le PA est porté par le protocole de PB).

Bien que le diagramme montre trois protocoles en couches, il est envisagé que le PA soit probablement une enveloppe de message mince autour d'un ensemble d'attributs et qu'il soit regroupé et encapsulé dans le PB. Le PB est principalement un protocole léger de traitement par lots de messages, de sorte que la pile de protocoles est principalement le transport (PT). Les lignes verticales dans le modèle représentent les API et/ou les protocoles entre les composants au sein du client ou serveur NEA. Ces interfaces sortent du domaine de normalisation du groupe de travail NEA.

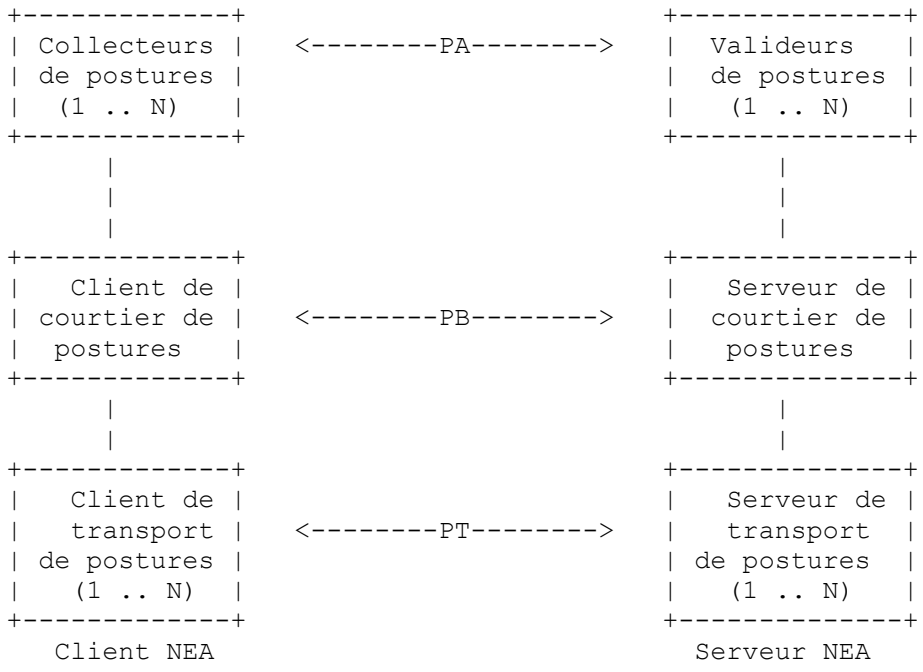

Figure 1 : Modèle de référence NEA

Le modèle de référence NEA n'inclut pas de mécanisme de découverte des clients et des serveurs NEA. On s'attend à ce que les clients et les serveurs NEA soient configurés avec des informations qui leur permettent de se joindre mutuellement. Les méthodes spécifiques de référencement de la configuration et d'établissement du canal de communication sortent du champ d'application du modèle de référence NEA et devraient être couvertes dans les spécifications des protocoles candidats tels que le protocole de transport de posture (PT, *Posture Transport*).

5.1 Client et serveur NEA

5.1.1 Client NEA

Le client NEA est résidant sur un appareil de point d'extrémité et comporte les fonctions suivantes :

- collecteur de postures
- client de courtier de posture
- client de transport de postures

Le client NEA est chargé de répondre aux demandes des attributs qui décrivent la configuration du domaine d'exploitation local du client et de traiter les résultats de l'évaluation, y compris les instructions de correction potentielles sur la façon de

se conformer à la politique. Un client NEA n'est pas chargé de rapporter sur la posture des entités qui pourraient exister sur le point d'extrémité ou sur le réseau, qui sont en dehors du domaine d'exécution (par exemple, dans d'autres domaines de machine virtuelle) du client NEA.

Par exemple, un appareil de traduction d'adresses réseau (NAT) pourrait acheminer les communications de nombreux systèmes derrière lui, mais lorsque l'appareil de NAT rejoint le réseau, son client NEA va seulement rapporter sa propre posture (locale). De même, les points d'extrémité dotés de capacités de virtualisation peuvent avoir plusieurs domaines d'exécution indépendants (par exemple, des instances de système d'exploitation). Chaque client NEA n'est responsable que de rapporter la posture pour son domaine d'exécution, mais ces informations pourraient être agrégées par d'autres mécanismes locaux pour représenter la posture de plusieurs domaines sur le point d'extrémité. De tels mécanismes d'agrégation de postures sortent du domaine d'application de cette spécification.

Les points d'extrémité qui n'ont pas de logiciel de client NEA (ce qui sort du domaine de NEA) ou qui choisissent de ne pas fournir les attributs exigés par le serveur NEA pourraient être considérés comme non conformes. Le modèle NEA inclut des capacités de permettre au point d'extrémité de mettre à jour son contenu afin de devenir conforme.

5.1.1.1 Collecteur de posture

Le collecteur de posture est responsable de la réponse aux demandes d'informations de posture dans les attributs de demande provenant du serveur NEA. Le collecteur de posture est aussi responsable du traitement des décisions d'évaluation dans les attributs de résultat et les instructions de remédiation dans les attributs de remédiation. Un seul client NEA peut avoir plusieurs collecteurs de posture capables de collecter des attributs de posture standard et/ou spécifiques de fabricant pour des caractéristiques particulières du point d'extrémité. Des exemples incluent des collecteurs de posture qui fournissent des informations sur la version du système d'exploitation (OS, *Operating System*) et les niveaux de réparation, le logiciel anti-virus, et les mécanisms de sécurité sur le point d'extrémité comme un système de détection d'intrusion (IDS, *Intrusion Detection System*) fondé sur l'hôte ou un pare-feu.

Chaque collecteur de posture va être associé à un ou plusieurs identifiants qui lui permettent d'être spécifié comme destination dans un message PA. Le client de courtier de posture utilise ces identifiants pour acheminer les messages à ce collecteur. Un identifiant pourrait être dynamique (par exemple, généré par le client de courtier de posture au démarrage durant l'enregistrement) ou plus statique (par exemple, pré-alloué au collecteur de posture au moment de l'installation et passé au client de courtier de posture durant l'enregistrement) ou une fonction des messages d'attribut que le collecteur désire recevoir (par exemple, le type de message pour l'abonnement).

Le modèle NEA alloue les responsabilités suivantes au collecteur de posture :

- Consulter les politiques locales de confidentialité et de sécurité qui peuvent restreindre les informations qu'il est permis de divulguer à un certain serveur NEA.

- Recevoir les attributs de demande d'un valideur de posture et effectuer le traitement local exigé pour répondre de façon appropriée. Cela peut inclure :
  - de collecter les informations de posture associées pour des caractéristiques particulières du point d'extrémité et de retourner ces informations dans les attributs de posture ;
  - de mettre en mémoire tampon et reconnaître l'applicabilité des attributs récemment produits contenant des assertions réutilisables qui pourraient servir à prouver la conformité et retourner ces attributs au lieu des informations de posture.

- Recevoir des attributs contenant des instructions de remédiation sur la façon de mettre à jour les fonctionnalités du point d'extrémité. Cela pourrait exiger que le collecteur interagisse avec l'utilisateur, le propriétaire, et/ou un serveur de remédiation.

- De surveiller la posture de caractéristiques particulières sur le point d'extrémité pour des changements de posture qui exigent une notification au client de courtier de posture.

- De fournir la vérification cryptographique des attributs reçus du validateur et d'offrir une protection cryptographique aux attributs retournés.

La liste ci-dessus décrit la vue du modèle des responsabilités possibles du collecteur de posture. Noter que ce n'est pas un ensemble d'exigences sur ce que chaque mise en œuvre de collecteur de posture doit prendre en charge, ni une liste exhaustive de toutes les choses qu'un collecteur de posture peut faire.

5.1.1.2 Client de courtier de posture

Le client de courtier de posture est à la fois un multiplexeur et un démultiplexeur de message de PA. Le client de courtier de posture est chargé de démultiplexer le message de PB reçu du serveur NEA et de distribuer chaque message de PA encapsulé au ou aux collecteurs de posture correspondants. Le modèle permet aussi que la demande d'informations de posture soit pré-provisionnée sur le client NEA pour améliorer les performances en permettant au client NEA de rapporter une posture sans recevoir de demande pour des attributs particuliers du serveur NEA.

Le client de courtier de posture multiplexe aussi les réponses du ou des collecteurs de posture et les retourne au serveur NEA. Le client de courtier de posture construit un ou plusieurs messages de PB en utilisant le ou les messages de PA qu'il obtient du ou des collecteurs de posture impliqués dans l'évaluation. La quantité et l'ordre des messages de réponse du collecteur de posture (messages de PA) multiplexés dans les messages de réponse de PB peuvent être déterminés par le client de courtier de posture sur la base de nombreux facteurs incluant la politique ou les caractéristiques de transport du réseau sous -jacent (par exemple, la MTU). Un client NEA particulier va avoir un client de courtier de posture.

Le client de courtier de posture traite aussi la décision d'évaluation globale à partir du serveur de courtier de posture et peut interagir avec l'utilisateur pour communiquer la décision globale d'évaluation et aider à toutes les étapes nécessaires de remédiation.

Le modèle NEA alloue les responsabilités suivantes au client de courtier de posture :
- o Tenir un registre des collecteurs de posture connus et permettre aux collecteurs de posture de s'enregistrer et désenregistrer de façon dynamique.
- o Multiplexer et démultiplexer les messages d'attributs entre le serveur NEA et les collecteurs de posture pertinents.
- o Traiter les notifications de changement de posture provenant des collecteurs de posture et déclencher la réévaluation.
- o Fournir des notifications aux utilisateurs sur la décision globale d'évaluation et autres messages d'utilisateur envoyés par le serveur NEA.

5.1.1.3 Client de transport de posture

Le client de transport de posture est chargé d'établir un canal fiable de communication avec le serveur NEA pour le dialogue de messages entre le client NEA et le serveur NEA. Il pourrait y avoir plus d'un client de transport de posture sur un client NEA particulier supportant différents protocoles de transport (par exemple, 802.1X, VPN). Certains clients de transport de posture peuvent être configurés avec l'adresse du serveur de transport de posture approprié à utiliser pour un réseau particulier.

Le modèle NEA alloue les responsabilités suivantes au client de transport de posture :
- o Initier et maintenir le canal de communication avec le serveur NEA. Le client de transport de posture cache les détails du transporteur sous-jacent qui pourrait être un protocole de couche 2 ou de couche 3.
- o Fournir la protection cryptographique au dialogue de messages entre le client NEA et le serveur NEA.

5.1.2 Serveur NEA

Le serveur NEA comporte normalement les fonctions NEA suivantes :
- o valideur de postures
- o serveur de courtier de posture
- o serveur de transport de postures.

Les valideurs de posture pourraient être situés sur un serveur séparé du serveur de courtier de posture, exigeant que le serveur de courtier de posture traite avec les valideurs de posture locaux et distants.

5.1.2.1 Valideur de posture

Un valideur de posture est chargé de traiter les attributs de posture provenant du ou des collecteurs de posture correspondants. Un valideur de posture peut traiter les attributs de posture provenant d'un ou plusieurs collecteurs de posture et vice-versa. Le valideur de posture effectue l'évaluation de posture pour une ou plusieurs caractéristiques du point d'extrémité (par exemple, logiciel anti-virus) et crée le résultat et, si nécessaire, les instructions de remédiation, ou il peut choisir de demander des attributs supplémentaires à un ou plusieurs collecteurs.

Chaque valideur de posture va être associé à un ou plusieurs identifiants qui lui permettent d'être spécifié comme destination dans un message de PA. Le serveur de courtier de posture utilise cet identifiant pour acheminer les messages à ce valideur. Cet identifiant pourrait être dynamique (par exemple, généré par le serveur de courtier de posture au démarrage

durant l'enregistrement) ou plus statique (par exemple, pré-alloué à un valideur de posture au moment de l'installation et passé au serveur de courtier de posture durant l'enregistrement) ou une fonction des messages d'attribut que le valideur désire recevoir (par exemple, le type de message pour l'abonnement).

Les valideurs de posture peuvent être co-localisés sur le serveur NEA ou peuvent être hébergés sur un serveur séparé. Un serveur NEA particulier va probablement avoir besoin de traiter plusieurs valideurs de posture.

Le modèle NEA alloue les responsabilités suivantes au valideur de posture :
- o Demander les attributs au collecteur de posture. La demande peut inclure :
  - des attributs de demande qui indiquent au collecteur de posture d'aller chercher et fournir des attributs de posture pour une fonction particulière sur le point d'extrémité.
- o Recevoir des attributs du collecteur de posture. La réponse du collecteur de posture peut inclure :
  - des attributs de posture collectés pour la fonction demandée ;
  - des attributs d'assertion qui indiquent la résultat de conformité pour une évaluation antérieure.
- o D'attester la posture de caractéristiques de point d'extrémité sur la base des attributs reçus du collecteur.
- o De communiquer le résultat de l'évaluation de posture au serveur de courtier de posture.
- o De communiquer le résultat de l'évaluation de posture au collecteur de posture ; ce message d'attribut peut inclure :
  - des attributs de résultat qui communiquent le résultat de l'évaluation de posture ;
  - des attributs de remédiation qui communiquent les instructions de remédiation au collecteur de posture.
- o De surveiller les mises à jour hors bande qui déclenchent une réévaluation et exigent que des notifications soient envoyées au serveur de courtier de posture.
- o De fournir une protection cryptographique aux attributs envoyés au collecteur de posture et d'offrr la vérification cryptographique des attributs reçus du collecteur de posture.

La liste ci-dessus décrit la vue du modèle des responsabilités possibles du valideur de posture. Noter que ce n'est pas un ensemble d'exigences que chaque mise en œuvre de valideur de posture doit prendre en charge, ni une liste exhaustive de toutes les choses qu'un valideur de posture peut faire.

5.1.2.2 Serveur de courtier de posture

Le serveur de courtier de posture agit comme multiplexeur et démultiplexeur des messages d'attribut. Le serveur de courtier de posture analyse les messages de PB reçus du client NEA et les démultiplexe en messages de PA qu'il passe aux valideurs de posture associés. Le serveur de courtier de posture multiplexe les messages de PA (par exemple, les messages contenant (a) des attributs de demande provenant du ou des valideurs de posture pertinents) en un ou plusieurs messages de PB et les envoie au client NEA via le protocole de transport de posture. La quantité et l'ordre des réponses de valideur de posture (messages de PA) et la décision globale d'évaluation multiplexée dans le ou les messages de réponse de PB peuvent être déterminés par le serveur de courtier de posture sur la base de nombreux facteurs incluant la politique ou les caractéristiques du transport du réseau sous-jacent (par exemple, la MTU).

Le serveur de courtier de posture est aussi chargé de calculer la décision globale d'évaluation sur la base des résultats individuels d'évaluation de posture provenant des divers valideurs de posture. Cette décision globale d'évaluation est renvoyée au client NEA dans les attributs de résultat au sein d'un message de PB. Un serveur NEA particulier va avoir un serveur de courtier de posture, et ce serveur de courtier de posture va traiter tous les valideurs de posture locaux et distants.

Le modèle NEA alloue les responsabilités suivantes au serveur de courtier de posture :
- o Tenir un registre des valideurs de posture et permettre aux valideurs de posture de s'y enregistrer et désenregistrer.
- o Multiplexer et démultiplexer les messages de posture des et aux valideurs de posture pertinents.
- o Calculer la décision globale d'évaluation sur la base des résultats de l'évaluation de posture provenant des divers valideurs de posture et de la politique de conformité. Cette décision d'évaluation est envoyée au client de courtier de posture dans un message de PB.

5.1.2.3 Serveur de transport de posture

Le serveur de transport de posture est chargé d'établir un canal de communication fiable avec le client NEA pour le dialogue de messages entre le client NEA et le serveur NEA. Il pourrait y avoir plus d'un serveur de transport de posture sur un serveur NEA particulier pour prendre en charge différents protocoles de transport. Un serveur de transport de posture particulier va normalement traiter les demandes provenant de plusieurs clients de transport de posture et peut exiger que la configuration locale décrive comment joindre les clients NEA.

Le modèle NEA alloue les responsabilités suivantes au serveur de transport de posture :
- o Initier et maintenir un canal de communication avec, potentiellement, plusieurs clients NEA.

o Fournir la protection cryptographique du dialogue de messages entre le client NEA et le serveur NEA.

5.2 Protocoles

Le modèle de référence NEA inclut trois couches de protocoles (PA, PB, et PT) qui permettent l'échange d'attributs à travers le réseau. Bien que ces protocoles soient destinés à être utilisés ensemble pour tenir un rôle particulier dans le modèle, ils peuvent offrir des fonctionnalités qui se chevauchent. Par exemple, chaque protocole devrait être capable de protéger ses informations contre une attaque (voir plus d'informations au paragraphe 8.2).

5.2.1 Protocole d'attribut de posture (PA)

PA est un protocole qui porte un ou plusieurs attributs entre des collecteurs de posture et leur valideur de posture associé. Le protocole de PA est une enveloppe légère en mode message autour d'un ensemble d'attributs échangés. Cette enveloppe peut indiquer l'objet des attributs au sein du message. Certains des types de messages attendus incluent des demandes d'informations de posture (attributs de demande), des informations de posture sur le point d'extrémité (attributs de posture), les résultats d'une évaluation (attributs de résultat), des assertions de conformité réutilisables (attributs d'assertion), et des instructions pour remédier à des portions non conformes du point d'extrémité (attributs de remédiation). Le protocole de PA fournit aussi les exigences de codage et de protection cryptographique pour les attributs de posture.

5.2.2 Protocole de courtier de posture (PB, *Posture Broker*)

PB est un protocole qui porte des messages d'attribut agrégés entre les collecteurs de posture sur le client NEA et les valideurs de posture correspondants sur le serveur NEA impliqué dans une évaluation particulière. Le protocole de PB fournit une session permettant des dialogues de messages pour chaque évaluation. Cette session de PB est alors utilisée pour lier plusieurs demandes et réponses d'attribut de posture provenant des différents collecteurs de posture et valideurs de posture impliqués dans une évaluation particulière. Le protocole de PB peut aussi porter la décision globale d'évaluation dans l'attribut de résultat provenant du serveur de courtier de posture au client de courtier de posture. Le PB peut être utilisé pour porter des types de messages supplémentaires à utiliser par le client et le serveur de courtier de posture (par exemple, des informations sur les réglages d'interface préférés de l'utilisateur comme le langage).

5.2.3 Protocole de transport de posture (PT)

Le PT est un protocole de transport entre le client NEA et le serveur NEA chargé de porter les messages générés par le protocole de PB. Les protocoles de PT transportent les messages de PB durant la demande de connexion au réseau ou après que la connexité au réseau a été établie.

Dans les scénarios où une évaluation initiale doit se produire durant la connexion au réseau, le protocole de PT (par exemple, EAP dans 802.1X) peut avoir une utilisation contrainte du réseau, de sorte que les déploiements peuvent choisir de limiter la quantité et/ou la taille des attributs échangés. Le client et le serveur NEA devraient être capables de détecter quand une situation potentiellement contrainte existe avant l'évaluation fondée sur les propriétés du protocole réseau sous-jacent. En utilisant ces informations, la politique de NEA pourrait dicter quels aspects du point d'extrémité inclure dans l'évaluation initiale et potentiellement limiter les attributs de message de PA échangés. Cela pourrait être suivi par une réévaluation complète après que le point d'extrémité est placé dans le réseau. Autrement, les déploiements peuvent choisir de ne pas limiter leur évaluation en configurant leur technologie d'accès réseau à accorder temporairement une connexité IPIP restreinte avant l'évaluation et utiliser un transport fondé sur IP non contraint à forte bande passante durant l'évaluation. Certaines des contraintes qui peuvent exister pour les protocoles impliqués dans la phase de connexion au réseau incluent :

o de limiter la taille maximum d'unité de transmission (MTU) et la capacité de négocier de plus grandes MTU,
o l'incapacité d'effectuer plusieurs allers-retours,
o la non prise en charge du portage des attributs pour d'autres protocoles,
o des limitations de bande passante ou de forte latence empêchant les échanges de grandes quantités de données,
o l'incapacité des serveurs à initier des messages sauf durant la phase de connexion au réseau.

Le processus de choix du protocole de PT doit considérer l'impact du choix d'un PT particulier et de l'ensemble des protocoles sous-jacents sur les besoins du déploiement de PA et PB. Les PA et PB vont être choisis avant le PT de sorte que le PA et le PB doivent être connus. Certaines piles de protocoles sous-jacents peuvent être trop contraintes pour prendre en charge des évaluations adéquates de NEA durant la connexion au réseau.

Le protocole de PT fournit une livraison fiable des messages, l'authentification mutuelle, et la protection cryptographique pour les messages de PB comme spécifié par la politique locale.

5.3 Attributs

Le protocole de PA est chargé de l'échange des attributs entre un collecteur de posture et un valideur de posture. Le protocole de PB peut aussi porter les attributs de décision d'évaluation globale provenant du serveur de courtier de posture. Les attributs sont effectivement les "noms" de mot réservé de l'évaluation de posture. Le serveur NEA est seulement capable de demander les informations qui ont un attribut correspondant, limitant donc le type de posture qui peut être obtenue. Le groupe de travail NEA définira un ensemble commun (standard) des attributs dont on s'attend qu'ils soient largement applicables aux collecteurs de posture et donc utilisés pour une interopérabilité maximale, mais les collecteurs de posture peuvent prendre en charge des attributs spécifiques de fabricant supplémentaires quand nécessaire.

Selon le scénario de déploiement, l'objet des attributs échangés peut être différent (par exemple, des informations de posture plutôt qu'une affirmation de conformité). Ce paragraphe discute de l'origine et de la situation attendue résultant en l'utilisation de chaque classification des attributs dans un message de PA. Ces classifications ne sont pas destinées à imposer comment le groupe de travail NEA va spécifier les attributs quand il définira l'espace de nom ou le schéma des attributs.

5.3.1 Attributs normalement envoyés par le client NEA

- Attributs de posture : les attributs et valeurs envoyés pour rapporter des informations sur un aspect particulier (sur la base de la sémantique de l'attribut) du système. Ces attributs sont normalement envoyés en réponse aux attributs de demande provenant du serveur NEA. Par exemple, un ensemble d'attributs de posture pourrait décrire l'état du pare-feu fondé sur l'hôte (par exemple, si il fonctionne, le fabricant, la version). Le serveur NEA fonderait sa décision sur la comparaison de ce type d'attribut à sa politique.

- Attributs d'assertion : les attributs qui déclarent une conformité antérieure récente à la politique dans l'espoir d'éviter d'avoir à recollecter la posture et l'envoyer au serveur NEA. Des exemples d'assertions incluent (a) des attributs (d'état) fournis au serveur NEA décrivant une évaluation antérieure (par exemple, opaque au point d'extrémité, signé, éléments horodatés déclarant des résultats spécifiques) ou (b) des informations d'identité de client NEA utilisées par le serveur NEA pour localiser l'état sur des décisions antérieures (par exemple, mouchard lié au système). Cela pourrait être retourné au lieu de, ou en plus des, attributs de posture.

5.3.2 Attributs normalement envoyés par le serveur NEA

- Attributs de demande : attributs qui définissent les informations de posture spécifiques désirées par le serveur NEA. Ces attributs pourraient effectivement former un gabarit que le collecteur de posture remplit (sous réserve des restrictions de politique locale) avec les valeurs spécifiques correspondant à chaque attribut. Les attributs résultants sont normalement les attributs Posture ou Assertion provenant du client NEA.

- Attributs de résultat : attributs qui contiennent les décisions des valideurs de posture et/ou serveur de courtier de posture. Le niveau de détail fourni peut varier selon que les attributs individuels étaient conformes ou non d'après juste la décision d'évaluation globale.

- Attributs de remédiation : attributs qui expliquent au client NEA et à son utilisateur comment mettre à jour le point d'extrémité pour qu'il devienne conforme aux politiques du serveur NEA. Ces attributs sont envoyés quand la décision d'évaluation globale était que le point d'extrémité n'est pas actuellement conforme. Les attributs de remédiation et de résultat peuvent tous deux exister dans un message d'attribut de serveur NEA.

- Attributs d'assertion : attributs qui contiennent les assertions de conformité du serveur NEA à une politique pour une utilisation future par le client NEA. Voir les détails au paragraphe 5.3.1.

6. Cas d'utilisation

Cette section discute plusieurs des cas d'utilisation de NEA avec l'intention de décrire et lier collectivement l'espace de problème de NEA considéré. Les cas d'utilisation fournissent un contexte et la raison générale des exigences définies. Afin de faciliter la compréhension de chaque cas d'utilisation et de comment il se transpose en le modèle de référence, chaque cas d'utilisation va être accompagné d'un simple exemple et d'une discussion de comment cet exemple se rapporte aux protocoles NEA. Il devrait être souligné que les exemples fournis ne sont pas destinés à indiquer la seule approche du

traitement du cas d'utilisation mais sont plutôt inclus pour faciliter la compréhension de la façon dont les flux pourraient se produire et impacter les protocoles NEA.

On classe en gros les cas d'utilisation en deux catégories, chacune avec son propre ensemble d'événements déclencheurs :

évaluation initiale - évaluation initiale de la posture d'un point d'extrémité qui n'a pas été récemment évalué et donc n'est pas en possession d'une preuve valide qu'il devrait être considéré comme conforme. Cette évaluation pourrait être déclenchée par une demande de se joindre à un réseau, une demande d'utiliser un service, ou un désir de comprendre la posture d'un système.

réévaluation - évaluation de la posture d'un point d'extrémité qui a été évalué précédemment. Cette évaluation pourrait survenir pour diverses raisons incluant la reconnaissance par le client ou serveur NEA d'une occurrence affectant le point d'extrémité qui pourrait relever le niveau de risque du point d'extrémité. Cela pourrait être aussi simple que la réévaluation précédente du point d'extrémité a été faite il y a longtemps.

6.1 Hypothèses initiales

Une évaluation initiale se produit quand un événement de client ou serveur NEA se produit, qui cause l'évaluation de la posture du point d'extrémité pour la première fois. Les points d'extrémité ne se qualifient pas pour cette catégorie de cas d'utilisation si ils ont été évalués récemment et si le client ou serveur NEA a conservé son état (ou sa preuve d'état) que le point d'extrémité est conforme et donc n'a pas besoin d'avoir sa posture évaluée à nouveau.

6.1.1 Déclenché par connexion réseau ou demande de service

Ce cas d'utilisation se concentre sur les évaluations effectuées au moment où un point d'extrémité tente de se joindre à un réseau ou demande à utiliser un service qui exige une évaluation de posture. Ce cas d'utilisation est particulièrement intéressant parce qu'il permet au serveur NEA d'évaluer la posture d'un point d'extrémité avant de lui permettre d'accéder au réseau ou service.

Cette approche pourrait être utilisée pour aider à détecter les points d'extrémité qui ont des vulnérabilités connues et de faciliter leur réparation avant qu'ils soient admis sur le réseau et potentiellement exposés aux menaces sur le réseau.

Une variété de types d'actions de point d'extrémité pourrait résulter en cette classe d'évaluation. Par exemple, une évaluation pourrait être déclenchée par l'essai du point d'extrémité d'accéder à un service réseau très protégé (par exemple, financier ou serveur d'application HR) où des vérification de sécurité renforcées sont exigées. Un exemple mieux connu pourrait inclure de demander l'entrée d'un réseau qui exige des systèmes qu'il satisfassent à la politique de conformité. Cet exemple est discuté plus en détail au paragraphe suivant.

6.1.1.1 Exemple

Un employé IT qui revient de vacances amorce son ordinateur de bureau qui génère une demande de se joindre au réseau filaire de l'entreprise. La politique de sécurité du réseau exige que le système fournisse des informations de posture afin de déterminer si les caractéristiques de sécurité de l'ordinateur sont activées et à jour. L'ordinateur envoie ses informations de posture de ses correctifs, pare-feu, et anti-virus. Le serveur NEA détermine qu'il manque au système un correctif de sécurité récent conçu pour corriger une sérieuse vulnérabilité et le système est placé sur un réseau d'accès restreint. L'ordinateur suit les instructions de correction fournies et installe le correctif nécessaire. Plus tard, l'ordinateur demande à nouveau à se joindre au réseau et cette fois le plein accès lui est fourni au réseau d'entreprise après une évaluation complète.

6.1.1.2 Flux possibles et usage du protocole

Les flux de message typiques sont décrits ici d'après le modèle de référence NEA pour cet exemple de cas d'utilisation :

1. L'ordinateur de l'employé IT se connecte au réseau à travers une passerelle d'accès dans le réseau filaire de l'entreprise.

2. Le serveur de courtier de posture sur le serveur NEA a pour instruction d'évaluer le point d'extrémité qui se joint au réseau filaire.

3. Sur la base de la politique de conformité, le serveur de courtier de posture contacte les valideurs de posture de correctif de système d'exploitation, de pare-feu fondé sur l'hôte, et d'anti-virus pour demander la posture nécessaire. Chaque

valideur de posture crée un message PA contenant les attributs dont l'évaluation est désirée pour le système d'ordinateur.

4. Le serveur de courtier de posture agrège les messages PA provenant des valideurs de posture en un message de PB. Le serveur de courtier de posture passe le message de PB au serveur de transport de posture qui utilise le protocole PT pour envoyer le message de PB au client NEA sur l'odinateur de bureau.

5 Le client de transport de posture reçoit le message venant du serveur NEA et le passe au client de courtier de posture pour la livraison du message.

6. Le client de courtier de posture démultiplexe le message de PB et livre les messages PA avec les demandes d'attributs aux collecteurs de posture de pare-feu, de correctif de système d'exploitation, et d'anti-virus.

7. Chaque collecteur de posture impliqué consulte la politique locale de confidentialité pour déterminer quelles informations il est permis de divulguer et retourne ensuite les attributs demandés permis dans un message PA au client de courtier de posture.

8. Le client de courtier de posture agrège ces messages PA en un seul message de PB et l'envoie au serveur de courtier de posture en utilisant la session de client à serveur de transport de posture.

9. Le serveur de transport de posture fournit le message de PB au serveur de courtier de posture qui démultiplexe le message et envoie les attributs appropriés au valideur de posture correspondant.

10 Chaque valideur de posture compare les valeurs des attributs qu'il reçoit aux valeurs attendues définies dans sa politique.

11. Les valideurs de posture anti-virus et de pare-feu retournent les attributs au serveur de courtier de posture déclarant que l'ordinateur de bureau est conforme, mais le valideur de posture de correctif de système d'exploitation retourne qu'il n'est pas conforme. Le valideur de posture de correctif de système d'exploitation crée un message PA qui contient les attributs avec les instructions de correction en plus de l'attribut indiquant le résultat de non conformité.

12. Le serveur de courtier de posture agrège les messages PA et les envoie dans un message de PB au client de courtier de posture via le serveur de transport de posture et le client de transport de posture.

13. Le client de courtier de posture livre les messages PA avec les résultats provenant des divers valideurs de posture au collecteurs de posture en incluant le message PA qui contient les attributs avec les instructions de remède du système d'exploitation du collecteur de posture de correctif. Ce collecteur de posture interagit alors avec l'utilisateur pour télécharger et installer les correctifs nécessaires, éventuellement pendant que le point d'extrémité reste en quarantaine.

14. Quand la correction est achevée, les étapes 1 à 10 ci-dessus sont répétées (déclenchées par le client NEA qui répète sa demande de se joindre au réseau).

15. Cette fois, chaque valideur de posture impliqué (incluant le valideur de posture de correction du système d'exploitation) retourne un état conforme et le serveur de courtier de posture retourne un résultat conforme indiquant un succès global.

16. Le client de courtier de posture reçoit le résultat conforme et l'ordinateur de l'employé TI est mainteant sur le réseau.

6.1.1.3 Impact sur les exigences

Voici plusieurs aspects différents de l'exemple de cas d'utilisation qui ont potentiellement besoin d'être mis en facteurs dans les exigences.

- o évaluation de posture avant que le point d'extrémité soit permis sur le réseau
- o le point d'extrémité envoie des attributs contenant les informations de posture
- o le serveur NEA envoie les instructions de correction
- o le client NEA cause une réévaluation après la correction.

6.1.2 Déclenché par un point d'extrémité

Ce cas d'utilisation souligne qu'un point d'extrémité (éventuellement à la demande d'un utilisateur) peut souhaiter déclencher une évaluation de sa posture pour déterminer si son mécanisme de protection de la sécurité fonctionne et est à jour.

6.1.2.1 Exemple

Un étudiant va à la salle d'informatique pour travailler sur un projet. La salle d'informatique contient des systèmes partagés qui appartiennent à l'école et qui sont sur le réseau. Ces systèmes ont été antérieurement utilisés par d'autres étudiants de sorte que leur posture de sécurité est inconnue. L'étudiant souhaite vérifier si un système est actuellement en conformité avec les politiques de sécurité de l'école avant de commencer son travail, et demande donc une évaluation de posture. Le serveur NEA effectue une évaluation initiale du système et détermine qu'il est conforme mais que la protection anti-virus n'est pas activée. L'étudiant reçoit une réponse indiquant que le logiciel anti-virus du système est éteint mais qu'autrement, il est conforme à la politique de l'école. L'étudiant active le logiciel anti-virus, initie un examen, et lorsque il est fini décide de faire confiance au système pour son travail.

6.1.2.2 Flux possibles et usage de protocole

Les flux de messages suivants sont décrits par le modèle de référence NEA pour l'exemple de l'étudiant qui utilise le système partagé de la salle d'informatique :

1. L'étudiant déclenche le client de courtier de posture sur le système d'ordinateurs dans la salle d'informatique pour initier une évaluation de posture.

2. Le client de courtier de posture établit une session avec le serveur de courtier de posture qui cause le déclenchement d'une évaluation.

3. Le serveur de courtier de posture détecte la nouvelle session et consulte la politique pour déterminer les valideurs de posture à impliquer dans l'évaluation. Le serveur de courtier de posture décide d'employer plusieurs valideurs de posture incluant le valideur de posture anti-virus.

4. Les valideurs de posture impliqués créent des messages PA contenant des demandes d'attributs particuliers contenant des informations sur l'ordinateur de la salle informatique désirées sur la base de la politique de sécurité de l'école.

5. Le serveur de courtier de posture assemble un message de PB incluant chaque message PA provenant des valideurs de posture.

6. Le serveur de transport de posture envoie le message de PB au client de transport de posture où il est passé au client de courtier de posture.

7. Le client de courtier de posture sur l'ordinateur de l'étudiant démultiplexe les messages PA et les livre aux collecteurs de posture correspondants.

8. Les collecteurs de posture consultent la politique de confidentialité pour décider quelles informations partager avec le serveur. Si c'est permis, chaque collecteur retourne un message PA contenant la posture demandée au client de courtier de posture.

9. Le client de courtier de posture agrège les messages PA retournés dans un message de PB et le passe au client de transport de posture pour transmission au serveur de transport de posture.

10. Le serveur de courtier de posture sépare et distribue le collecteur de messages de posture PA aux valideurs de posture associés.

11. Les valideurs de posture déterminent si les attributs contenus dans la posture qui incluaient le message PA sont conformes à leurs politiques et retournent une décision d'évaluation de posture au serveur de courtier de posture. Dans ce cas, le valideur de posture anti-virus retourne un message PA indiquant un résultat non conforme parce que le logiciel anti-virus n'est pas activé et inclut des attributs décrivant comment activer le logiciel.

12. Le serveur de courtier de posture détermine la décision de conformité globale sur la base de tous les résultats d'évaluation des valideurs et envoie un message de PB contenant un attribut qui exprime la décision d'évaluation globale et le message PA du valideur anti-virus. Dans ce cas, la décision d'évaluation globale indique que le système est conforme (en dépit du résultat du valideur anti-virus) parce que la politique du serveur de courtier de posture permet que l'anti-virus ne soit pas activé pour autant que le système a été correctement corrigé et fait fonctionner un pare-feu (ce qui était le cas selon les autres valideurs de posture).

13. Le serveur de transport de posture envoie le message de PB au client de transport de posture qui fournit le message au client de courtier de posture.

14. Le client de courtier de posture sur l'ordinateur de la salle d'informatique examine l'attribut de la décision d'évaluation globale du message de PB et rapporte à l'étudiant que le système est réputé être conforme, mais qu'un conseil a été inclus.

15. Le client de courtier de posture fournit le message PA avec les attributs de remède au collecteur de posture anti-virus qui interagit avec l'utilisateur pour expliquer comment activer l'anti-virus afin d'améliorer les protections locales.

16. L'étudiant active le logiciel anti-virus et quand c'est fait les étapes 1 à 10 sont répétées.

17. Cette fois le valideur de posture anti-virus retourne un état de succès et le serveur de courtier de posture retourne une décision d'évaluation globale de succès dans le message de PB.

18. Le client de courtier de posture reçoit la décision d'évaluation globale de succès dans le message de PB et l'étudiant utilise maintenant l'ordinateur pour son allocation.

6.1.2.3 Impact sur les exigences

Voici plusieurs aspects différents de l'exemple de cas d'utilisation qui ont potentiellement besoin d'être mis en facteurs dans les exigences :

- le point d'extrémité volontaire a demandé l'évaluation initiale,
- la décision d'évaluation globale de succès (conforme) est incluse dans le message de PB avec un message PA contenant un ensemble d'attributs de correction pour information.

6.2 Réévaluation de posture

La réévaluation des points d'extrémité peut se produire à tout moment après l'admission au réseau suite à une évaluation initiale NEA réussie. Ces réévaluations peuvent être fondées sur des événements, comme des changements de posture détectés par le client NEA, ou sur des changements détectés par l'infrastructure de réseau, tels qu'un comportement suspect ou des mises à jour de la politique du réseau sur le serveur NEA. Elles peuvent aussi être périodiques (conduites par un temporisateur) pour réévaluer la santé du point d'extrémité.

6.2.1 Déclenché par le client NEA

Ce cas d'utilisation permet au logiciel sur le point d'extrémité ou un utilisateur de déterminer qu'une réévaluation du système est exigée. Il y a diverses raisons pour qu'une telle réévaluation pourrait être bénéfique, incluant des changements de la posture rapportée pécédemment, la détection de comportements potentiellement suspects, ou même de permettre au système d'interroger périodiquement le serveur NEA pour évaluer sa condition par rapport aux dernières politiques.

6.2.1.1 Exemple

Les ordinateurs de bureau du département ressources humaines d'une entreprise ont une histoire de mauvaises pratiques de sécurité et même de compromission. L'administrateur du département de ressources humaines décide de déployer un logiciel sur chaque ordinateur pour surveiller l'utilisation des mécanismes de protection de la sécurité pour assurer leur usage. Un jour, un employé des ressources humaines débranche accidentellement le pare-feu de son ordinateur. Le processus de surveillance détecte le manque de pare-feu et contacte le serveur NEA pour demander une réévaluation de la conformité du pare-feu. Le serveur NEA retourne une décision qui dit que le pare-feu doit être réactivé pour rester sur le réseau. Le client NEA explique la décision à l'utilisateur et comment réactiver le pare-feu. L'employé des ressources humaines redémarre le pare-feu et initie une demande pour rejoindre le réseau.

6.2.1.2 Flux possibles et usage de protocole

Les flux de messages suivants sont décrits avec le modèle de référence NEA pour l'exemple du département des ressources humaines :

1. Le logiciel de surveillance d'ordinateur qui pourrait normalement agir comme un collecteur de posture déclenche l'initiation par le courtier de posture du client d'une évaluation de posture. Le client de courtier de posture crée un message de PB qui contient un message PA indiquant que le pare-feu de l'ordinateur a été désactivé.

2. Le client de courtier de posture envoie le message de PB au serveur de courtier de posture.

3. Le client de transport de posture envoie le message de PB au serveur de transport de posture sur le protocole PT.

4. Le serveur de courtier de posture reçoit le message de PB et transmet le message de PA au pare-feu valideur de posture pour évaluation.

5. Le pare-feu valideur de posture détermine que le point d'extrémité n'est plus conforme parce que son pare-feu a été désactivé.

6. Le valideur de posture génère un message PA qui contient des attributs indiquant un résultat d'évaluation de posture non conforme et des instructions de correction sur la façon de réactiver le pare-feu.

7. Le valideur de posture communique le message PA avec le résultat de l'évaluation de posture au serveur de courtier de posture pour qu'il réponde au client NEA.

8. Le serveur de courtier de posture génère un message de PB incluant une décision d'évaluation globale de non conformité et le message PA provenant du pare-feu valideur de posture.

9. Le serveur de transport de posture transporte le message de PB au client de transport de posture où il est passé au client de courtier de posture.

10. Le client de courtier de posture traite l'attribut contenant la décision d'évaluation globale reçue du serveur NEA et affiche les messages de non conformité à l'utilisateur.

11. Le client de courtier de posture transmet le message PA au pare-feu collecteur de posture ; le collecteur de posture affiche les instructions de correction sur la façon d'activer le pare-feu de l'ordinateur.

12. L'utilisateur est invité à initier une réévaluation après avoir achevé la correction.

13. À l'achèvement de la correction, le client NEA réinitie une demande de réévaluation et les étapes 1 à 4 sont répétées. Cette fois le pare-feu valideur de posture détermine que le point d'extrémité est conforme et retourne une décision d'évaluation de posture de succès.

14. Le serveur de courtier de posture génère un message de PB avec une décision d'évaluation globale de conformité et la retourne au client NEA.

6.2.1.3 Impact sur les exigences

Ce qui suit sont plusieurs différents aspects d'exemple de cas d'utilisation qui ont potentiellement besoin d'être pris en compte dans les exigences.

- Volontairement, le point d'extrémité (son logiciel) a initié une demande de réévaluation de posture
- Le serveur NEA demande des attributs de posture spécifiques dépendants du pare-feu
- Le client NEA (pare-feu collecteur de posture) interagit avec l'utilisateur pour remédier au problème.

6.2.2 Déclenché par le serveur NEA

Dans de nombreux cas, en particulier pour les réévaluations, le serveur NEA peut initier des réévaluations spécifiques ou complètes d'un ou plusieurs points d'extrémité déclenchées par :

- l'heure (périodique)
- l'occurrence d'un événement
- la mise à jour de la politique

6.2.2.1 Exemple

Une entreprise exige des employés sur le réseau qu'ils restent toujours à jour des corrections critiques pour la sécurité du système d'exploitation. Un employé du service commercial se joint au réseau et effectue une évaluation initiale. L'évaluation détermine que l'ordinateur de l'employé est conforme. Plusieurs heures après, un fabricant majeur du système d'exploitation livre un ensemble de correctifs prévenant une sérieuse vulnérabilité qui est exploitée sur l'Internet.

Les administrateurs de l'entreprise rendent les correctifs disponibles et changent la politique du réseau pour exiger qu'ils soient installés avant 17 heures. Ce changement de politique cause la demande par le serveur NEA d'une réévaluation pour déterminer quels points d'extrémité sont impactés et n'ont pas les correctifs. L'ordinateur de l'employé du service commercial est réévalué et est déterminé avoir besoin des correctifs. Un avis de remède est envoyé et présenté à l'employé, expliquant comment obtenir les correctifs et disant qu'ils doivent être installés pour 17 heures. L'employé du service commercial télécharge et installe immédiatement les correctifs et obtient l'assertion que tous les correctifs sont maintenant installés.

À 17 heures, l'entreprise effectue une autre réévaluation de tous les points d'extrémité impactés pour déterminer si ils sont maintenant conformes. L'ordinateur de l'employé du service commercial est réévalué et présente l'assertion qu'il a les correctifs installés et donc est déterminé être conforme.

6.2.2.2 Flux possibles et usage de protocole

On décrit maintenant les flux de messages à travers le modèle de référence NEA pour l'exemple ci-dessus :

1. L'employé du service commercial se joint au réseau et réalise une évaluation initiale résultant en une décision de conformité.

2. L'administrateur de l'entreprise configure un correctif de politique du système d'exploitation qui indique que les correctifs récents sont exigés sur tous les points d'extrémité pour 17 heures pour prévenir de sérieuses vulnérabilités.

3. Le valideur de posture de correctifs du système d'exploitation du serveur NEA est averti de ce changement de politique et crée un message PA qui demande les attributs décrivant les correctifs de l'OS à utiliser et déclenche l'initiation par le serveur de courtier de posture d'une réévaluation de posture de tous les points d'extrémité connectés au réseau.

4. Le courtier de posture crée un message de PB qui inclut le message PA provenant du valideur de posture de correctifs du système d'exploitation.

5. Le serveur de courtier de posture établit graduellement une session avec chaque client NEA disponible.

6. Le serveur de courtier de posture envoie le message de PB au client de courtier de posture.

7. Le serveur de transport de posture porte le message de PB au client de transport de posture sur le protocole PT.

8. Le client de courtier de posture reçoit le message de PB et transmet le message PA au collecteur de posture de correctifs du système d'exploitation.

9. Le collecteur de posture de correctifs du système d'exploitation détermine les correctifs d'OS présents sur le point d'extrémité et si il y est autorisé par sa politique de divulgation, il crée un message PA contenant les attributs d'informations de correctifs.

10. Le client de courtier de posture envoie un message de PB qui inclut le message PA de correctifs du système d'exploitation.

11. Le client de transport de posture transporte le message de PB au serveur de transport de posture où il est passé au serveur de courtier de posture.

12. Le serveur de courtier de posture reçoit le message de PB et livre le message PA au valideur de posture de correctifs du système d'exploitation.

13. Le valideur de posture de correctifs du système d'exploitation extrait les attributs décrivant les correctifs d'OS actuels du message PA et utilise les valeurs pour déterminer si le point d'extrémité est conforme à la nouvelle politique. Le valideur de posture détermine que le point d'extrémité n'est pas conforme car il n'a pas installé les nouveaux correctifs d'OS.

14. Le valideur de posture génère un message PA qui inclut les attributs déclarant la décision d'évaluation de posture non conforme et les attributs contenant les instructions de correction pour permettre au point d'extrémité de télécharger les correctifs d'OS exigés.

15. Le valideur de posture communique les résultats de l'évaluation de posture au serveur de courtier de posture avec son message PA.

16. Le serveur de courtier de posture génère une décision d'évaluation globale et envoie un message de PB avec la décision et le message PA du valideur de posture de correctifs du système d'exploitation.

17. Le serveur de transport de posture transporte le message de PB au client de transport de posture où il est passé au client de courtier de posture.

18. Le client de courtier de posture traite l'attribut de résultat reçu du serveur NEA et affiche la décision de non conformité à l'utilisateur.

19. Le client de courtier de posture transmet le message PA contenant les instructions de correction au collecteur de posture de correctifs du système d'exploitation ; le collecteur de posture guide l'utilisateur avec des instructions sur la façon de devenir conforme qui incluent de télécharger les correctifs d'OS appropriés pour empêcher la vulnérabilité.

20. L'employé du service commercial installe les correctifs exigés et est maintenant conforme.

21. Le client NEA déclenche une réévaluation des correctifs du système d'exploitation qui cause la répétition de beaucoup des étapes ci-dessus. Cette fois, dans l'étape 13, le valideur de posture de correctifs du système d'exploitation détermine que l'ordinateur de l'employé du service commercial est conforme. Il retourne un ensemble réutilisable d'attributs (par exemple, signés et datés) qui affirment la conformité des correctifs d'OS à la dernière politique. Ces attestations de conformité de correctifs d'OS peuvent être utilisés dans un futur message PA provenant du collecteur de correctifs du système d'exploitation au lieu de déterminer et fournir la posture d'ensemble de correctifs spécifique comme précédemment.

22. Cette fois, quand le collecteur de posture de correctifs du système d'exploitation reçoit le message PA qui contient les attributs réutilisables attestant de la conformité, il met ces attributs en antémémoire pour une utilisation future.

23. Après 17 heures, le serveur NEA déclenche une réévaluation graduelle pour déterminer la conformité à l'avis de correction. Quand le collecteur de posture de correctifs du système d'exploitation reçoit la demande d'informations de posture (comme dans l'étape 9 ci-dessus) il retourne l'ensemble d'assertions mis en antémémoire (au lieu des informations de correctif spécifiques de l'OS) pour indiquer que les correctifs ont bien été installés au lieu de déterminer tous les correctifs qui ont été installés sur le système.

24. Quand le valideur de posture de correctifs du système d'exploitation reçoit le message PA contenant les assertions, il est capable de déterminer qu'elles sont authentiques et acceptables au lieu d'une posture spécifique. Il retourne une décision d'évaluation de posture conforme permettant donc à l'ordinateur de rester sur le réseau.

6.2.2.3 Impact sur les exigences

Voici plusieurs aspects différents de l'exemple de cas d'utilisation qui doivent potentiellement être pris en compte dans les exigences.

- Les réévaluations initiées par le serveur exigées du fait de l'urgence de la disponibilité des correctifs
- Le client NEA soumet les attributs d'assertion réutilisables au lieu de la posture que le correctif est installé
- Le serveur NEA est capable de reconnaître que les attributs d'assertion précédemment fournis sont suffisants plutôt que la posture.

7. Exigences

Cette Section décrit les exigences qui vont être utilisées par le groupe de travail NEA pour valider et comparer les protocoles candidats pour PA, PB, et PT. Ces exigences expriment fréquemment des caractéristiques qu'un protocole candidat doit être capable d'offrir afin qu'un déploiement puisse décider d'utiliser cette caractéristique. Cette section ne déclare pas les exigences sur les caractéristiques que chaque protocole doit utiliser durant un déploiement.

Par exemple, une exigence (DOIT, DEVRAIT, ou PEUT) pourrait exister pour que des protections de sécurité cryptographique soient disponibles dans chaque protocole mais cela n'exige pas qu'un déploiement les utilise toutes ou même certaines si il devait estimer que son environnement offre d'autres protections qui sont suffisantes.

7.1 Exigences communes de protocole

Ci-après figurent les exigences communes qui s'appliquent aux protocoles de PA, PB, et PT dans le modèle de référence NEA :

C-1 Les protocoles NEA DOIVENT prendre en charge plusieurs allers-retours entre le client NEA et le serveur NEA dans une seule évaluation.

C-2 Les protocoles NEA DEVRAIENT fournir un moyen pour que le client NEA et le serveur NEA initient une évaluation ou réévaluation de posture comme nécessaire.

C-3 Les protocoles NEA qui incluent des capacités de sécurité DOIVENT être capables de se protéger contre des attaques actives et passives de la part d'intermédiaires et de points d'extrémité incluant la prévention d'attaques fondées sur la répétition.

C-4 Les protocoles PA et PB DOIVENT être capables de fonctionnner sur tout protocole de PT. Par exemple, le protocole PB doit fournir une interface indépendante du transport permettant au protocole de PA de fonctionner sans changement à travers divers environnements de protocole réseau (par exemple, EAP/802.1X, TLS, et le protocole d'échange de clé Internet de version 2 (IKEv2)).

C-5 Le processus de sélection des protocoles NEA DOIT évaluer et préférer la réutilisation des normes ouvertes existantes qui satisfont les exigences plutôt que d'en définir de nouvelles. Le but de NEA n'est pas de créer des protocoles de remplacement supplémentaires lorsque des solutions acceptables existent déjà.

C-6 Les protocoles NEA DOIVENT être très adaptables ; les protocoles DOIVENT prendre en charge de nombreux collecteurs de posture sur un grand numbre de clients NEA pour être évalués par de nombreux valideurs de posture résidant sur plusieurs serveurs NEA.

C-7 Les protocoles DOIVENT prendre en charge le transport efficace d'un grand nombre de messages d'attributs entre le client NEA et le serveur NEA.

C-8 Les protocoles NEA DOIVENT opérer efficacement sur des liaisons à faible bande passante ou à forte latence.

C-9 Pour toute chaîne destinée à l'affichage à un utilisateur, les protocoles DOIVENT prendre en charge l'adaptation de ces chaînes aux préférence de langage de l'utilisateur.

C-10 Les protocoles NEA DOIVENT prendre en charge le codage des chaînes en format UTF-8 [RFC3629].

C-11 Du fait des caractéristiques de transport potentiellement différentes fournies par les protocole PT candidats sous-jacents, le client NEA et le serveur NEA DOIVENT être capables de s'informer des, et s'adapter aux limitations du protocole PT disponible. Par exemple, certaines caractéristiques de protocole PT qui pourraient impacter le fonctionnement de PA et PB incluent des restrictions sur quelle extrémité peut initier une connexion NEA, la taille maximum de données dans un message ou une évaluation complète, une limite supérieure au nombre d'allers-retours, et l'ordre (en duplex) des messages échangés. Le processus de choix des protocoles PT DOIT considérer les limitations que le protocole PT candidat imposerait aux protocoles PA et PB.

7.2 Exigences pour le protocole d'attribut de posture (PA)

Le protocole d'attribut de posture (PA) définit le modèle de transport et de données pour porter les informations de posture et de validation entre un collecteur de posture particulier associé au client NEA et un valideur de posture associé au serveur NEA. Le protocole de PA porte des collections d'attributs standard et d'attributs spécifiques du fabricant. Le protocole de PA lui-même est porté dans le protocole PB.

Les exigences suivantes définissent les propriétés désirées qui forment la base de comparaison et d'évaluation des protocoles PA candidats. Ces exigences ne rendent pas obligatoire l'utilisation de ces propriétés, mais simplement que les protocoles candidats sont capables d'offrir la propriété si elle devait être nécessaire.

PA-1 Le protocole de PA DOIT prendre en charge la communication d'un ensemble extensible d'attributs définis par les normes NEA. Ces attributs vont être distingués des attributs non standard.

PA-2 Le protocole de PA DOIT prendre en charge la communication d'un ensemble extensible d'attributs spécifiques des fabricants. Ces attributs vont être segmentés en espaces de noms spécifiques de fabricant identifiés de façon univoque.

PA-3 Le protocole de PA DOIT permettre à un valideur de posture de faire une ou plusieurs demandes d'attributs à un collecteur de posture dans une seule évaluation. Cela permet au valideur de posture de réévaluer la posture d'une caractéristique particulière d'un point d'extrémité ou de demander une posture supplémentaire incluant d'autres parties du point d'extrémité.

PA-4 Le protocole de PA DOIT être capable de retourner des attributs provenant d'un valideur de posture à un collecteur de posture. Par exemple, cela pourrait permettre au collecteur de posture d'apprendre la raison de l'échec d'une évaluation, d'aider à y remédier, et d'en notifier le propriétaire du système.

PA-5 Le protocole de PA DEVRAIT fournir l'authentification, la protection de l'intégrité et de la confidentialité pour les attributs communiqués entre un collecteur de posture et un valideur de posture. Cela permet la sécurité de bout en bout à travers le déploiement NEA qui pourrait impliquer la traversée de plusieurs systèmes ou frontières de confiance.

PA-6 Le protocole de PA DOIT être capable de porter des attributs qui contiennent des données non binaires et binaires incluant du contenu chiffré.

7.3 Exigences pour le protocole de courtier de posture (PB)

Le protocole de PB prend en charge le multiplexage des messages d'attribut de posture (sur la base du protocole de PA) entre les collecteurs de posture sur le client NEA de et vers les valideurs de posture sur le serveur NEA (dans l'une et l'autre direction).

Le protocole PB porte la décision d'évaluation globale faite par le serveur de courtier de posture, prenant en compte les résultats des valideurs de posture impliqués dans l'évaluation, au client de courtier de posture.

Le protocole de PB agrège aussi et transporte des avis et notifications telles que des instructions de correction (par exemple, les références des corrections) provenant d'un ou plusieurs valideurs de posture.

Les exigences pour le protocole de PB sont :

PB-1 Le protocole PB DOIT être capable de porter des attributs du serveur de courtier de posture au client de courtier de posture. Cela permet au client de courtier de posture d'apprendre les décisions d'évaluation de posture et si c'est approprié d'aider à y remédier et en notifier le propriétaire du point d'extrémité.

PB-2 Le protocole PB NE DOIT PAS interpréter les contenus des messages PA portés, c'est-à-dire, les données qu'il porte doivent lui être opaques.

PB-3 Le protocole PB DOIT porter des identifiants univoques qui sont utilisés par les courtiers de posture pour acheminer (livrer) les messages PA entre les collecteurs de posture et les valideurs de posture. Un tel acheminement de messages devrait faciliter l'enregistrement ou désenregistrement dynamique des collecteurs et valideurs de posture. Par exemple, un valideur de posture dynamiquement enregistré d'anti-virus devrait être capable de s'abonner à la réception de messages provenant des collecteurs de posture anti-virus respectifs sur les clients NEA.

PB-4 Le protocole PB DOIT être capable de prendre en charge un protocole PT unidirectionnel. Cependant cela n'empêche pas le PB d'opérer en bi-directionnel quand il fonctionne sur un PT bi-directionnel.

PB-5 Le protocole PB PEUT prendre en charge l'authentification, la protection de l'intégrité et de la confidentialité pour les messages d'attribut qu'il porte entre un client de courtier de posture et un serveur de courtier de posture. Cela fournit la protection de la sécurité d'un dialogue de messages des groupements de messages d'attributs échangés entre le client de courtier de posture et le serveur de courtier de posture. Une telle protection est orthogonale aux protections de PA (qui sont de bout en bout) et permet de mettre en œuvre des collecteurs et valideurs de posture plus simples, et la consolidation d'opérations cryptographiques améliorant éventuellement l'adaptabilité et la gérabilité.

PB-6 Le protocole de PB DOIT prendre en charge le groupement des messages d'attribut pour optimiser le transport des messages et minimiser le nombre d'allers-retours.

7.4 Exigences pour le protocole de transport de posture (PT)

Le protocole de transport de posture (PT, *Posture Transport*) porte les messages de protocole de PB entre le client de transport de posture et le serveur de transport de posture. Le PT est chargé de fournir un transport protégé pour le protocole PB. Le protocole PT peut lui-même être transporté par une ou plusieurs sessions enchaînées en utilisant des protocoles de couche inférieure, comme 802.1X, RADIUS [RFC2865], TLS, ou IKE.

Ce paragraphe définit les exigences que les protocoles PT candidats doivent être capables de prendre en charge.

PT-1 Le protocole PT NE DOIT PAS interpréter les contenus des messages PB transportés, c'est-à-dire, les données qu'il porte doivent lui être opaques.

PT-2 Le protocole PT DOIT être capable de prendre en charge l'authentification mutuelle, la protection de l'intégrité, de la confidentialité, et contre la répétition des messages PB entre le client de transport de posture et le serveur de transport de posture.

PT-3 Le protocole PT DOIT fournir une livraiosn fiable pour le protocole PB. Cela inclut la capacité d'effectuer la fragmentation et le réassemblage, la détection des dupliqués, et de réordonner pour fournir la livraison en séquence, comme exigé.

PT-4 Le protocole PT DEVRAIT être capable de fonctionner sur les protocoles existants d'accès réseau comme 802.1X et IKEv2.

PT-5 Le protocole PT DEVRAIT être capable de fonctionner entre un client NEA et un serveur NEA sur TCP ou UDP (similaire au protocole léger d'accès à un répertoire (LDAP)).

8. Considérations sur la sécurité

Le présent document définit les exigences fonctionnelles pour les protocoles PA, PB, et PT utilisés pour l'évaluation de point d'extrémité de réseau (NEA, *Network Endpoint Assessment*). À ce titre, il ne définit pas une pile de protocoles spécifique ni un ensemble de technologies, donc cette section va souligner les problèmes de sécurité qui peuvent s'appliquer à NEA en général ou à des aspects particuliers du modèle de référence NEA.

Noter que bien qu'un certain nombre de sujets soient en dehors du mandat du groupe de travail NEA et donc de la présente spécification (voir le paragraphe 3.1) il est important que ces mécanismes soient protégés des attaques. Par exemple, les méthodes de déclenchement d'une évaluation ou réévaluation sortent du domaine d'application mais devraient être protégées de façon appropriée contre les attaques (par exemple, un attaquant cachant l'événement qui indique qu'un changement de politique d'un serveur NEA s'est produit).

NEA est destiné à faciliter la détection et les actions correctives pour que des points d'extrémité coopérants deviennent conformes aux politiques de conformité du réseau. Par exemple, il est envisagé que ces politiques permettent aux déployeurs de détecter des mécanismes de sécurité périmés, inactifs, ou absents sur le point d'extrémité qui pourraient le laisser plus vulnérable à des attaques connues. Si un point d'extrémité est plus vulnérable à la compromission, il est alors plus risqué d'avoir ce point d'extrémité présent sur le réseau avec d'autres actifs de valeur. En évaluant de façon proactive les points d'extrémité coopérants avant leur entrée dans le réseau, les déployeurs peuvent améliorer leur résilience aux attaques avant l'accès au réseau. De même, les réévaluations des points d'extrémité coopérants sur le réseau peuvent être utiles en assurant que les mécanismes de sécurité restent utilisés et sont à jour avec les dernières politiques.

NEA reconnaît pleinement que tous les points d'extrémité ne vont pas coopérer en fournissant leur posture valide (ou aucune posture du tout). Cela pourrait se produire si un malgiciel influence le client NEA ou les politiques, et donc une évaluation digne de confiance n'est pas possible. Une telle situation pourrait résulter en l'admission d'un point d'extrémité qui introduit des menaces pour le réseau et autres points d'extrémité en dépit de la réussite de l'évaluation de conformité NEA.

8.1 Confiance

L'évaluation de point d'extrémité réseau implique d'évaluer la posture des points d'extrémité entrants ou déjà sur le réseau par rapport aux politiques de conformité pour assurer qu'ils sont adéquatement protégés. Donc, il doit y avoir une défiance

implicite à l'égard des points d'extrémité jusqu'à ce qu'il y ait des raisons de croire (sur la base des informations de posture) qu'ils sont protégés contre les menaces visées par la politique de conformité et peuvent être de confiance pour ne pas propager ces menaces aux autres points d'extrémité. Du côté du fournisseur du réseau, le client NEA est normalement supposé faire confiance aux systèmes d'infrastructure du réseau pour ne pas mésuser des informations de posture divulguées (voir la Section 9) et de toutes les instructions de correction fournies au point d'extrémité. Le client NEA a normalement aussi besoin de faire confiance au serveur NEA pour seulement demander les informations exigées pour déterminer si le point d'extrémité est sûr pour accéder aux actifs du réseau.

Entre le client NEA et le serveur, il existe un réseau qui n'est pas supposé être de confiance. Donc, la confiance dans le réseau est implicitement limitée à la confiance dans sa volonté et capacité de transporter les messages échangés en temps utile. La quantité de confiance accordée à chaque composant du modèle de référence NEA est spécifique du déploiement. Le groupe de travail NEA à l'intention de fournir des mécanismes de sécurité pour réduire la quantité de confiance qui doit être supposée par un déployeur. Les paragraphes qui suivent discutent chaque domaine plus en détail.

8.1.1 Point d'extrémité

Pour que NEA fonctionne correctement, le point d'extrémité doit être de confiance pour représenter de façon précise la posture de sécurité demandée du point d'extrémité au serveur NEA. Selon le mandat du groupe de travail NEA, le modèle de référence NEA ne spécifie pas explicitement comment détecter ou prévenir le mensonge des points d'extrémité qui intentionnellement représentent mal leur posture. De même, la détection de malgiciels (par exemple, des ensembles racines) qui sont capables de tromper les collecteurs de posture en retournant des informations incorrectes est l'objet de recherches et de normalisation en dehors de l'IETF (par exemple, Trusted Computing Group [TCG]) et n'est pas spécifiquement traité par le modèle. Cependant, si de tels mécanismes sont utilisés dans un déploiement, le modèle de référence NEA devrait être capable de s'accommoder de ces technologies en leur permettant de communiquer sur le PA avec les valideurs de posture ou de travailler perpendiculairement pour protéger le client NEA des attaques et assurer la capacité des collecteurs de posture de voir la posture réelle.

À côté de la confiance dans l'intégrité du client NEA et de sa capacité de collecter et rapporter précisément les attributs de posture sur le point d'extrémité, on essaye de limiter la confiance supposée par ailleurs. La plupart des modèles d'usage pour NEA s'attendent à ce que les informations de posture soient envoyées au serveur NEA pour qu'il fasse l'évaluation et la prise de décision. Quand des protections de sécurité de niveau PA et/ou PT sont utilisées, le point d'extrémité a besoin de faire confiance à l'intégrité et potentiellement la confidentialité des informations de l'ancre de confiance (par exemple, des certificats de clé publique) utilisées par le collecteur de posture et/ou le client de transport de posture. Cependant, les mises en œuvre NEA peuvent choisir d'envoyer ou pré-provisionner certaines politiques au point d'extrémité pour une évaluation qui supposerait plus de confiance dans le point d'extrémité. Dans ce cas, le serveur NEA doit faire confiance à la mémorisation de politique, à l'évaluation et aux mécanismes de rapport du point d'extrémité pour ne pas falsifier les résultats de l'évaluation de posture.

Généralement, le point d'extrémité ne devrait pas faire confiance aux communications du réseau (par exemple, des demandes de connexion entrantes) sauf si cette confiance a été spécifiquement autorisée par la politique ou action définie par l'utilisateur ou le propriétaire. Le modèle de référence NEA suppose que le client NEA entier est local pour le point d'extrémité. Les communications non sollicitées originaires du réseau devraient être inspectées par les mécanismes normaux de protection de la sécurité fondés sur l'hôte (par exemple, des pare-feu, des protocoles de sécurité, un système de prévention/détection d'intrusion (IDS/IPS, *Intrusion Detection/Prevention System*) etc.). Les communications associées à une évaluation ou réévaluation NEA exigent un certain niveau de confiance en particulier quand elles sont initiées par le serveur NEA (réévaluation). Le degré de confiance peut être limité par l'utilisation de fortes protections de sécurité sur les messages comme dicté par le déployeur du réseau et la politique de l'utilisateur/propriétaire du point d'extrémité.

8.1.2 Communications de réseau

Entre le client et le serveur NEA, il peut exister divers types d'appareils pour faciliter le chemin de communication. Certains des appareils peuvent servir d'intermédiaires (par exemple, de simples commutateurs de couche 2) de sorte qu'ils peuvent avoir l'opportunité d'observer et changer les dialogues de messages.

Les appareils intermédiaires peuvent entrer dans quelques catégories majeures qui impactent notre degré de confiance dans leur fonctionnement. D'abord, certains appareils intermédiaires peuvent agir comme transmetteurs ou transporteurs de messages pour le PT (par exemple, commutateurs de couche 2, routeurs de couche 3). Pour ces appareils, on leur fait confiance pour ne pas éliminer les messages ou tenter activement de perturber (par exemple, un déni de service) le déploiement de NEA.

Ensuite, certains appareils intermédiaires peuvent faire partie de la couche de contrôle d'accès du réseau et à ce titre, on leur fait confiance pour appliquer les politiques de remédiation, d'isolation, et les contrôles d'accès qui leur sont donnés par suite d'une évaluation NEA. Ces appareils peuvent aussi tenir d'autres types de rôles décrits dans ce paragraphe.

Troisièmement, certains appareils peuvent agir comme point de terminaison ou mandataire pour le protocole de transporteur PT. Fréquemment, il est attendu que le protocole transporteur pour PT se termine sur le client et le serveur NEA de sorte qu'ils vont être co-résidents avec les points d'extrémité PT. Si cette attente n'est pas présente dans un déploiement, on doit faire confiance à l'appareil de terminaison pour transmettre précisément par délégation les messages PT sans altération au protocole de transporteur suivant (par exemple, si des messages de méthode EAP interne transitent d'un tunnel EAP [RFC3748] à une session RADIUS).

Quatrièmement, de nombreux réseaux incluent une infrastructure comme des appareils IDS/IPS qui surveillent et prennent une action corrective quand un comportement suspect est observé sur le réseau. Ces appareils peuvent avoir une relation avec le serveur NEA qui sort du domaine d'application de la présente spécification. Les appareils auxquels le serveur NEA fait confiance pour fournir des informations de sécurité qui pourraient affecter les décisions du serveur NEA sont de confiance pour fonctionner correctement et ne pas causer de prise de décisions incorrectes par le serveur NEA.

Finalement, d'autres types d'appareils intermédiaires peuvent exister sur le réseau entre le client et le serveur NEA qui sont présents pour servir à d'autres fonctions du réseau en dehors de NEA. Ces appareils pourraient être capables d'espionner passivement sur le réseau, archivant les informations pour des objets futurs (par exemple, répétition ou invasion de la vie privée) ou attaquer plus activement les protocoles NEA. Parce que ces appareils ne jouent pas de rôle de facilitation dans NEA, il est essentiel que les déployeurs de NEA ne soient pas forcés de leur faire confiance pour que NEA fonctionne de façon fiable. Donc, il est exigé que les protocoles NEA offrent des protections de sécurité pour assurer que ces appareils ne peuvent pas voler, altérer, usurper ou autrement endommager la fiabilité des dialogues de messages.

8.1.3 Serveur NEA

Le serveur NEA (incluant des systèmes potentiellement distants qui fournissent des services de validation de posture) est généralement de confiance pour appliquer les politiques d'évaluation spécifiées et doivent être protégés de la compromission. Il est essentiel que les déploiements de serveur NEA sauvegardent de façon appropriée ces systèmes de diverses attaques provenant du réseau et des points d'extrémité pour assurer leur fonctionnement approprié.

Bien qu'il soit nécessaire d'accorder un certain degré de confiance au fonctionnement du serveur NEA, une architecture de sécurité rigoureuse, l'analyse, la surveillance, et la révision devraient assurer que l'empreinte du réseau et son fonctionnement interne sont protégés des attaques. L'empreinte du réseau inclurait les communications sur le réseau qui pourraient être soumises à des attaques comme le provisionnement de politique à partir des systèmes d'auteur de politique et les protocoles de sécurité générale et de gestion de système. Des exemples de fonctionnement interne incluent des protections contre des malgiciels qui attaquent les communications intra serveur NEA, la logique interne du serveur NEA, ou les magasins de politiques (en particulier ceux qui changeraient les décisions ou applications résultantes). Le serveur NEA a besoin de faire confiance aux protocoles NEA sous-jacents et de réseau de couche inférieure pour se comporter de façon appropriée et sauvegarder les messages échangés avec le point d'extrémité. Le modèle de référence NEA ne tente pas de traiter de la protection de l'intégrité du système d'exploitation ou d'autre logiciel qui prend en charge le serveur NEA.

Un exemple intéressant est quand certains composants du serveur NEA résident physiquement dans des systèmes différents. Cela pourrait arriver quand un valideur de posture (ou un serveur d'extrémité distante utilisé par un valideur de posture local) existe sur un autre système à partir du serveur de courtier de posture. De même, le serveur de courtier de posture pourrait exister sur un système séparé du serveur de transport de posture. Quand il y a une séparation physique, les communications entre les composants distants du serveur NEA doivent s'assurer que la session de PB et les dialogues de messages de PA sont résistants aux attaques actives et passives, en particulier, gardés contre l'espionnage, la falsification et la répétition. De même, les valideurs de posture peuvent aussi souhaiter minimiser leur confiance dans le serveur de courtier de posture au delà de sa capacité d'envoyer et livrer correctement les messages PA. Les valideurs de posture pourraient employer la sécurité PA de bout en bout pour vérifier l'authenticité et protéger l'intégrité et/ou la confidentialité des messages PA échangés.

Quand la sécurité PA est utilisée, chaque valideur de posture doit être capable de faire confiance à l'intégrité et potentiellement la confidentialité de ses politiques d'ancre de confiance.

8.2 Mécanismes de protection à plusieurs couches

Inhérent aux exigences est le désir que les protocoles NEA candidats dans le modèle de référence soient capables de fournir de forts mécanismes de sécurité comme demandé par les déploiements particuliers. Dans certains cas, ces mécanismes

peuvent apparaître fournir des protections redondantes ou qui se chevauchent . Ces chevauchements apparents peuvent être utilisés en combinaison pour offrir une défense en profondeur de l'approche de la sécurité. Cependant, à cause de la mise en couches des protocoles, chaque ensemble de protections offre des avantages et des niveaux de granularité légèrement différents.

Par exemple, un déployeur peut souhaiter chiffrer le trafic à la couche PT pour protéger contre certaines formes d'analyse de trafic ou son interception par un espion. De plus, le déployeur peut aussi chiffrer sélectivement les messages qui contiennent la posture d'un point d'extrémité pour réaliser la confidentialité de bout en bout avec son valideur de posture correspondant. En particulier, cela pourrait être désiré quand le valideur de posture n'est pas co-localisé avec le serveur NEA de sorte que les informations vont traverser des segments de réseau supplémentaires après que les protections de PT ont été appliquées ou afin que le valideur de posture puisse authentifier le collecteur de posture correspondant (ou vice versa).

Différents cas d'utilisation et environnements pour les technologies de NEA vont probablement influencer le choix de la force et des mécanismes de sécurité employés durant une évaluation. Le but des exigences NEA est d'encourager le choix de technologies et protocoles qui soient capables de fournir les protections nécessaires pour une large gamme de types d'évaluation.

8.3 Classes d'attaques pertinentes

Diverses attaques sont possibles contre les protocoles NEA et les technologies d'évaluation. Ce paragraphe n'inclut pas une analyse complète de la sécurité, mais souhaite souligner quelques attaques qui ont influencé la définition des exigences et devraient être prises en compte par les déploiements qui choisissent d'utiliser les mécanismes de protection du modèle de référence NEA.

Comme expliqué, il y a divers mécanismes de protection qui sont inclus dans les exigences pour les protocoles NEA candidats. Différents cas d'utilisation et environnements peuvent amener les déploiements à décider de ne pas utiliser certains de ces mécanismes ; cependant, cela devrait être fait en comprenant que le déploiement peut devenir vulnérable à certaines classes d'attaques. Comme toujours, un compromis entre risque et performances, utilisabilité, gérabilité, et autres facteurs devrait être pris en compte.

Les types d'attaques suivants sont applicables aux protocoles réseau définis dans le modèle de référence et devraient donc être considérés par les déploiements.

8.3.1 Attaque par interposition

Les attaques par interposition (MITM, *Man-in-the-Middle*) contre un protocole réseau existent quand un tiers peut s'insérer entre deux entités communicantes sans détection et tirer parti de leur engagement dans leur dialogue de messages. Par exemple, un système infesté par un malgiciel pourrait souhaiter se joindre au réseau en répétant la posture observée d'un point d'extrémité propre qui entre dans le réseau. Cela pourrait se produire avec le système qui s'insère lui-même dans un dialogue de messages d'évaluation et joue un rôle actif de mandataire dans ce dialogue. L'impact de dommages causé par le MITM peut être limité ou empêché par le choix de mécanismes appropriés de protection du protocole.

Par exemple, l'exigence que le PT soit capable de prendre en charge l'authentification mutuelle avant tout dialogue de message d'évaluation de point d'extrémité empêche l'attaquant de s'insérer lui-même comme participant actif (mandataire) dans les communications sans détection (en supposant que l'attaquant n'a pas d'accréditifs convainquant l'une et l'autre partie qu'il est légitime). Des accréditifs réutilisables ne devraient pas être exposés sur le réseau pour s'assurer que le MITM n'a pas de moyen de se faire passer pour l'une ou l'autre des parties. L'exigence que le PT ait des communications protégées quant à la confidentialité (chiffrées) liée à l'authentification ci-dessus empêche un MITM passif d'espionner en observant le dialogue de messages et en gardant un enregistrement des valeurs de posture conformes pour une utilisation future. L'exigence de PT de prévention de la répétition arrête l'essai d'un MITM passif d'établir plus tard une nouvelle session (ou d'en capturer une existante) et de réexécuter les dialogues de messages précédemment observés.

Si un MITM non conforme actif est capable de tromper un point d'extrémité propre à abandonner ses informations de posture, et si le MITM a des accréditifs légitimes, il pourrait être capable d'apparaître à un serveur NEA comme ayant une posture conforme quand il ne l'a pas. Par exemple, un MITM non conforme pourrait se connecter et s'authentifier à un serveur NEA et lorsque le serveur NEA demande des informations de posture, le MITM pourrait demander la même posture au point d'extrémité propre. Si le point d'extrémité propre fait confiance au MITM pour effectuer une réévaluation et accepte de partager la posture demandée, le MITM pourrait obtenir la posture nécessaire du point d'extrémité propre et l'envoyer au serveur NEA. Afin de traiter cette forme d'attaque par interposition, les protocoles NEA auront besoin d'offrir un lien fort (cryptographique) entre les informations de posture et la session authentifiée au serveur NEA afin que celui-ci

sache que la posture a pour origine le point d'extrémité qui s'est authentifié. Un tel lien fort entre l'origine de la posture et le point d'extrémité qui s'authentifie peut être faisable et devrait être préféré par le groupe de travail NEA.

8.3.2 Modification de message

Sans protection de l'intégrité du message, un attaquant capable d'intercepter un message pourrait être capable de modifier son contenu et de causer la prise d'une décision incorrecte. Par exemple, l'attaquant pourrait changer les attributs de posture pour refléter toujours des valeurs incorrectes et donc empêcher un système conforme de se joindre au réseau. Sauf si le serveur NEA peut détecter ce changement, l'attaquant pourrait empêcher l'admission d'un grand nombre de systèmes corrects. À l'inverse, l'attaquant pourrait permettre à une machine infestée par un malgiciel d'être admise en changeant les attributs de posture envoyés pour refléter des valeurs conformes, cachant donc le malgiciel au valideur de posture. L'attaquant pourrait aussi infecter des points d'extrémité conformes en envoyant des instructions de correction malveillantes qui, quand elles sont effectuées, introduiraient le malgiciel sur le point d'extrémité ou désactiveraient les mécanismes de sécurité.

Afin de se protéger contre de telles attaques, le PT inclut une exigence de forte protection de l'intégrité (par exemple, en incluant un hachage protégé comme un code d'authentification de message haché (HMAC, *Hashed Message Authentication Code*) [RFC2104] du message) de sorte que tout changement à un message serait détecté. PA inclut une exigence similaire pour permettre la protection de bout en bout de l'intégrité des attributs, étendant la protection tout le long du chemin au valideur de posture même si il est situé sur un autre système derrière le serveur NEA.

Il est important que les schémas de protection de l'intégrité s'appuient sur des informations de secret fraîches (non connues de l'attaquant) qui sont liées à la session authentifiée comme par un HMAC utilisant un secret frais dérivé associé à la session. L'inclusion des informations de fraîcheur permet aux parties de se protéger contre certaines formes d'attaques en répétition de message qui utilisent les informations secrètes provenant de sessions antérieures.

8.3.3 Répétition de message ou vol d'attribut

Un attaquant pourrait écouter sur le réseau, enregistrant les dialogues ou attributs de message provenant d'un point d'extrémité conforme pour une réutilisation ultérieure au même serveur NEA ou juste pour construire un inventaire des logiciels fonctionnant sur d'autres systèmes pour trouver des vulnérabilités connues. Le serveur NEA doit être capable de détecter la répétition de posture et/ou le modèle doit assurer que l'espion ne peut pas obtenir les informations en premier lieu. Pour cette raison, il est exigé du protocole PT qu'il fournisse la confidentialité et la prévention de la répétition.

La protection cryptographique contre la divulgation des messages PT, PB, ou PA empêche l'écouteur passif d'observer les messages échangés et empêche donc le vol des informations pour une utilisation future. Cependant, un attaquant actif pourrait être capable de répéter le message chiffré si il n'y a pas un lien fort à la partie ou session d'origine. En liant le dialogue de messages chiffré à l'événement d'authentification et en s'appuyant sur la fraîcheur par transaction et les échanges chiffrés, cela empêche une répétition de la transaction chiffrée.

8.3.4 Autres types d'attaques

Ce paragraphe ne prétend pas présenter une liste exhaustive des attaques contre le modèle de référence NEA. Plusieurs types d'attaques vont devenir plus faciles à comprendre et analyser une fois que le groupe de travail NEA aura créé les spécifications qui décrivent les technologies et protocoles spécifiques à utiliser dans NEA. Une de ces zones est le déni de service (DoS). Pour l'instant, il n'est pas pratique d'essayer de définir toutes les expositions potentielles présentes dans les protocoles NEA, de sorte qu'une telle analyse devrait être incluse dans les sections de considérations sur la sécurité des protocoles NEA choisis.

Cependant, il est important que le serveur NEA soit résiliant aux attaques de DoS car une panne pourrait affecter un grand nombres de points d'extrémité souhaitant se joindre ou rester sur le réseau. Le modèle de référence NEA s'attend à ce que le protocole PT ait une certaine résilience au DoS et que les protocoles PA et PB aient besoin de construire ses propres protections sur ces bases. Pour aider à réduire la fenêtre d'attaque par des parties non authentifiées, il est envisagé que les serveurs NEA emploient les protocoles PT qui permettent une authentification mutuelle précoce du point d'extrémité demandeur comme technique de filtrage des attaques.

Les attaques qui surviennent après l'authentification vont au moins provenir de sources possédant des accréditifs valides et pouvant potentiellement être tenues pour valables. De même, les protocoles NEA devrait offrir une forte protection contre la répétition pour prévenir les attaques fondées sur le DoS sur des sessions et messages répétés. L'évaluation de posture devrait être fortement liée aux authentifications de transport de posture qui se sont produites pour s'assurer que la posture vient de la partie authentifiée. Des mécanismes cryptographiques et d'autres opérations potentiellement grosses

consommatrices de ressources devraient être utilisés avec parcimonie jusqu'à ce que la validité de la demande puisse être établie. Cela et d'autres attaques fondées sur les ressources/protocoles peut être évalué une fois que les technologies de NEA et leur utilisation cryptographique ont été choisies.

9. Considérations de confidentialité

Bien qu'il y ait un certain nombre d'avantages à l'utilisation de la technologie NEA pour les organisations qui possèdent et font fonctionner des réseaux offrant des services à des points d'extrémité également possédés, ces mêmes technologies pourraient augmenter le potentiel d'abus et d'invasion de la confidentialité personnelle si elles sont détournées. Cette Section va discuter quelques uns des problèmes potentiels de confidentialité soulevés par le déploiement de cette technologie et offrir des lignes directrices aux mises en œuvre.

La technologie NEA permet une plus grande visibilité sur la configuration d'un point d'extrémité vue du réseau. Une telle transparence permet au réseau de prendre en considération la force des mécanismes de sécurité du point d'extrémité quand il prend des décisions de contrôle d'accès aux ressources du réseau. Cependant, cette transparence pourrait aussi être utilisée pour appliquer des politiques restrictives au détriment de l'utilisateur en limitant son choix de logiciels ou en fouillant dans les utilisations passées ou présentes du point d'extrémité.

Le mandat du groupe de travail NEA était limité à spécifier des protocoles visant les cas d'utilisation où les points d'extrémité et le réseau sont possédés par la même partie ou où le possesseur du point d'extrémité a établi une attente claire de divulgation/conformité avec le propriétaire du réseau. C'est un modèle familier pour les gouvernements, institutions, et une grande variété d'entreprises qui fournissent des points d'extrémité à leurs employés pour effectuer leurs tâches. Dans beaucoup de ces situations, le point d'extrémité est possédé par l'entreprise et se réserve souvent le droit d'examen et éventuellement impose les utilisations admises de l'appareil. Les technologies de NEA leur permettent d'automatiser l'inspection des contenus d'un point d'extrémité et cette information peut être reliée aux mécanismes de contrôle d'accès sur le réseau pour limiter l'utilisation du point d'extrémité si celui-ci ne satisfait pas le niveau minimum de conformité.

Dans ces environnements, le niveau de confidentialité personnelle de l'employé peut être significativement réduit selon les lois et coutumes locales. Cependant, dans des situations où le point d'extrémité est possédé par l'utilisateur ou où les lois locales protègent les droits de l'utilisateur même quand il utilise des points d'extrémité possédés par un tiers, il est critique que la mise en œuvre de NEA permette à l'utilisateur de contrôler quelles informations de point d'extrémité sont partagées avec le réseau. De tels contrôles imposés par l'utilisateur pourraient empêcher ou limiter leur capacité d'accéder à certains réseaux ou ressources protégées, mais ceci doit être un choix de l'utilisateur.

9.1 Considérations de mise en œuvre

Le groupe de travail NEA ne définit pas de norme de contenu de politique de client NEA ni d'exigences sur les aspects d'une mise en œuvre en dehors des protocoles de réseau ; cependant, les lignes directrices suivantes sont fournies pour encourager les mises en œuvre favorables à la confidentialité à une utilisation plus large que juste les réglages d'entreprise décrits ci dessus.

Les mises en œuvre de client NEA sont encouragées à offrir une politique d'inscription aux utilisateurs avant de partager leurs informations de posture de point d'extrémité. Le mécanisme d'inscription devrait être par utilisateur, par serveur NEA afin que chaque utilisateur puisse contrôler quels réseau peut accéder à toutes les informations de posture sur son système. Pour les réseaux à qui il est permis d'accéder au point d'extrémité, l'utilisateur devrait être capable de spécifier des restrictions de granularité sur les types particuliers et les attributs spécifiques de collecteurs de posture à qui il est permis de divulguer. Il est déconseillé aux mises en œuvre de valideur de posture d'avoir le comportement par défaut d'utiliser des demandes à caractères génériques pour la posture conduisant potentiellement à une surexposition des informations (voir le paragraphe 9.2). Les valideurs de posture devraient plutôt par défaut seulement demander que des attributs spécifiques soient exigés pour effectuer leur évaluation.

Les demandes d'attributs dont le partage n'est pas explicitement permis (ou spécifiquement interdit) devraient résulter en une notification à l'utilisateur et/ou un enregistrement afin que l'utilisateur puisse évaluer si le service fait quelque chose d'indésirable ou si l'utilisateur veut partager ces informations supplémentaires pour obtenir l'accès. Certains produits pourraient considérer une prise en charge pilotée par la politique pour inviter l'utilisateur à autoriser qu'une description spécifique des informations de posture soit demandée avant de les envoyer au serveur NEA.

Il est envisagé que le propriétaire du point d'extrémité soit capable de spécifier les politiques de divulgation qui peuvent outrepasser ou influencer les politiques de l'utilisateur sur les attributs visibles au réseau. Si la politique de divulgation du propriétaire permet une disponibilité de posture plus large que la politique de l'utilisateur, la mise en œuve devrait fournir

un mécanisme de rétroaction aux utilisateurs afin qu'ils comprennent la situation et puissent choisir si ils utilisent le point d'extrémité dans ces circonstances.

Dans un tel système, il est important que l'interface d'auteur de politique de l'utilisateur soit facile à comprendre et articule clairement la politique de divulgation actuelle du système incluant toutes les influences de la politique du propriétaire. Les utilisateurs devraient être capables de comprendre quelle posture est disponible au réseau et que l'impact général de ces informations soit connu. Afin de minimiser la liste des restrictions énumérées, l'utilisation d'une politique de divulgation par défaut prudente telle que "ce qui n'est pas explicitement autorisé à être divulgué n'est pas permis" pourrait avoir un sens pour éviter des fuites involontaires d'informations.

Les mises en œuvre de serveur NEA devraient fournir aux points d'extrémité nouvellement abonnés une déclaration de divulgation qui dise clairement :
o quelles informations sont exigéés
o comment ces informations vont être utilisées et protégées
o quelles politiques de confidentialité locales sont applicables.

Ces informations vont permettre aux utilisateurs qui s'abonnent de décider si la divulgation de ces informations est acceptables selon les lois et coutumes locales.

9.2 Minimiser la divulgation d'attribut

Une question importante dans la conception du modèle de référence et des protocoles NEA est de permettre aux points d'extrémité de divulguer les informations minimales exigées pour établir la conformité aux politiques du réseau. Il y a plusieurs modèles qui pourraient être considérés sur comment est établi l'ensemble des attributs divulgués. Chaque modèle a des avantages à l'égard de la confidentialité et des questions qui devraient être considérées par les développeurs de produits. Ce paragraphe résume trois modèles potentiels sur la façon dont la divulgation d'attribut pourrait être fournie dans les produits de NEA et des implications de confidentialité potentiellement associées à chaque modèle.

Le premier modèle est facile à mettre en œuvre et déployer mais a des implications de confidentialité et potentiellement de latence et d'adaptabilité. Cette approche est effectivement par défaut que la politique locale envoie tous les attributs de posture NEA connus quand une évaluation se produit. Bien que cela pourrait simplifier le déploiement, cela expose beaucoup d'informations qui sont potentiellement non pertinentes pour l'évaluation de la sécurité du système et peut introduire des problèmes de confidentialité. Par exemple, est il réellement important que l'entreprise sache si Firefox est utilisé sur un système plutôt que d'autres navigateurs durant l'évaluation de posture de sécurité ?

Le second modèle implique un provisionnement hors bande de la politique de divulgation à tous les points d'extrémité. Ce modèle peut impliquer que l'entreprise établisse une politique selon laquelle une liste particulière d'attributs doit être fournie quand un échange NEA se produit. La politique de confidentialité des points d'extrémité peut filtrer cette liste d'attributs, mais de tels changements pourraient causer le non accès du point d'extrémité au réseau ou aux ressources. Ce modèle simplifie l'échange du réseau car le point d'extrémité envoie toujours la liste filtrée des attributs quand elle est mise au défi par un réseau particulier. Cependant, cette approche exige un protocole de gestion hors bande pour établir et gérer les politiques de divulgation NEA de tous les systèmes.

Le troisième modèle évite d'avoir besoin de pré-provisionner la politique de divulgation en permettant au serveur NEA de demander spécifiquement quels attributs sont exigés. Ceci est un peu analogue au provisionnement de la politique durant les échanges de NEA et est donc beaucoup plus facile à gérer. Ce modèle permet au serveur NEA de demander de façon itérative les attributs sur la base des valeurs des attributs antérieurs. Noter que même dans ce modèle, les protocoles NEA ne sont pas supposés être un langage d'interrogation d'objet général, mais permettent plutôt au serveur NEA de demander des attributs spécifiques car il est seulement possible de demander les attributs définis. Par exemple, une entreprise pourrait demander la version d'OS dans le dialogue de messages initial et après avoir appris que le système fonctionne avec Linux demander un ensemble différent d'attributs spécifiques de Linux de ce qu'elle aurait demandé si le point d'extrémité avait été un système Windows. Il est envisagé que cette approche pourrait minimiser l'ensemble d'attributs envoyés sur le réseau si l'évaluation est celle d'un système complexe (comme d'essayer de comprendre quels correctifs manquent à un OS).

Dans chaque modèle, l'utilisateur pourrait créer un ensemble de politiques de filtre de confidentialité par réseau appliquées par le client NEA pour empêcher la divulgation des attributs perçus comme étant de nature personnelle ou non pertinents pour un réseau particulier. De tels filtres protégeraient la confidentialité de l'utilisateur mais pourraient résulter en ce que l'utilisateur ne soit pas admis à accéder aux ressources (ou réseau) désirées ou n'ait qu'un accès limité.

10. Références

10.1 Références normatives

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

10.2 Références pour information

[802.1X] "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control", IEEE Std 802.1X-2001, juin 2001.

[CNAC] Cisco, Cisco's Network Admission Control Main Web Site, http://www.cisco.com/go/nac

[NAP] Microsoft, Network Access Protection Main Web Site, http://www.microsoft.com/nap

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.S.)*

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

[TCG] Trusted Computing Group, Main TCG Web Site, http://www.trustedcomputinggroup.org/

[TNC] Trusted Computing Group, Trusted Network Connect Main Web Site, https://www.trustedcomputinggroup.org/groups/network/

11. Remerciements

Les auteurs de ce document tiennent à remercier les membres du groupe de travail NEA qui ont contribué aux précédents documents de déclaration des exigences et de position de problème qui ont influencé la direction de la présente spécification : Kevin Amorin, Parvez Anandam, Diana Arroyo, Uri Blumenthal, Alan DeKok, Lauren Giroux, Steve Hanna, Thomas Hardjono, Tim Polk, Ravi Sahita, Joe Salowey, Chris Salter, Mauricio Sanchez, Yaron Sheffer, Jeff Six, Susan Thompson, Gary Tomlinson, John Vollbrecht, Nancy Winget, Han Yin, et Hao Zhou.

Adresse des auteurs

Paul Sangster
Symantec Corporation
6825 Citrine Dr
Carlsbad, CA 92009 USA
téléphone : +1 760 438-5656
mél : Paul_Sangster@symantec.com

Hormuzd Khosravi
Intel
2111 NE 25th Avenue
Hillsboro, OR 97124 USA
téléphone : +1 503 264 0334
mél : hormuzd.m.khosravi@intel.com

Mahalingam Mani
Avaya Inc.
1033 McCarthy Blvd.
Milpitas, CA 95035 USA
téléphone : +1 408 321-4840
mél : mmani@avaya.com

Kaushik Narayan
Cisco Systems Inc.
10 West Tasman Drive
San Jose, CA 95134
téléphone : +1 408 526-8168
mél : kaushik@cisco.com

Joseph Tardo
Nevis Networks
295 N. Bernardo Ave., Suite 100
Mountain View, CA 94043 USA
mél : joseph.tardo@nevisnetworks.com

Déclaration complète de droits de reproduction