CISCO
SECURE

Livre blanc
Document public de Cisco

La vérification systématique à grande échelle

Table des matières

Introduction

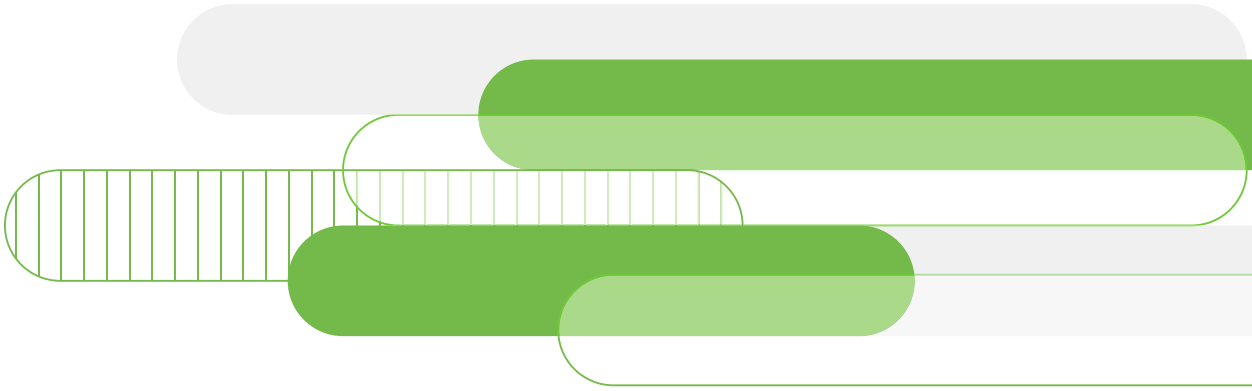
En 2020, Cisco a entrepris de passer d'un modèle traditionnel de périmètre de réseau et de RPV à un cadre à vérification systématique. Surnommé « sans frontières » à l'interne, l'objectif principal était de donner aux utilisateurs une expérience sécurisée et uniforme d'accès aux applications, où que se trouve l'utilisateur ou l'application. En utilisant les fonctionnalités de Duo Beyond, notre équipe a entrepris d'améliorer la sécurité et de créer une meilleure expérience pour nos plus de 100 000 utilisateurs, un changement fondamental qui s'est produit en moins de cinq mois.

À quoi ressemble la vérification systématique chez Cisco?

Lorsque nous pensons à la vérification systématique chez Cisco, quatre choses doivent se produire chaque fois que quelqu'un essaie d'accéder à une application :

1. Nous vérifions l'utilisateur
2. Nous confirmons que l'appareil est à jour et que son intégrité est intacte
3. Nous validons qu'un appareil géré par Cisco est utilisé
4. Il est possible d'accéder à l'application sans RPV

Et quand nous disons chaque fois, nous sommes sérieux. Pas une fois par jour, pas pour une seule application, mais en continu.



Pourquoi choisir l'approche à vérification systématique?

Prenons d'abord un peu de recul et expliquons pourquoi l'approche à vérification systématique est importante. Une solution de sécurité moderne est essentielle pour suivre le rythme d'un paysage des menaces qui évolue.

Identité	Application	Environnement
Selon le rapport d'enquête sur les violations de données de Verizon de 2022, 82 % des violations comprenaient « l'élément humain », soit par l'utilisation d'informations d'identification volées, d'escroqueries par hameçonnage (pour voler des informations d'identification), d'erreurs et d'une mauvaise utilisation des ressources. Ce rapport laisse entendre que les mots de passe restent une cible pour les agresseurs, et rendre l'accès sécurisé facile pour les utilisateurs est un moyen efficace de réduire les risques.[1]	Plus de 50 % de tous les sites Web mondiaux étaient vulnérables à au moins une vulnérabilité exploitable grave tout au long de l'année.[2] L'omniprésence croissante des logiciels-services (SaaS) et le déplacement de données précieuses vers le nuage, y compris les comptes de messagerie et les processus commerciaux, signifient que les applications non sécurisées peuvent être une invitation cachée à l'exploitation.	L'IDC prévoit qu'il y aura près de 56 milliards d'appareils connectés dans le monde d'ici 2025, dont 75 % seront connectés à une plateforme d'Internet des objets. Ces appareils intelligents, bien qu'utiles, peuvent être une cible à risque pour les agresseurs qui souhaitent accéder à votre réseau.

1 : Source : https://www.verizon.com/business/resources/reports/dbir/
2 : Source : https://www.whitehatsec.com/blog/appsec-stats-flash-2021-year-in-review/

De plus, nous savons que les vulnérabilités et leur exploitation continuent d'être les causes premières de la plupart des violations de la sécurité de l'information. Bien que les jours zéro reçoivent beaucoup d'attention, ils ne représentent historiquement que 0,4 % des vulnérabilités. En fait, les vulnérabilités non surveillées et non corrigées pendant des mois, voire des années, sont les vecteurs les plus courants. Bon nombre d'entre elles peuvent être évitées simplement en gardant les appareils à jour avec des correctifs logiciels et des mises à jour du système d'exploitation. Par conséquent, la validation de l'intégrité de l'appareil (c'est-à-dire s'il est à jour et corrigé) devient très importante lors de la décision d'autoriser ou non l'accès à une ressource.

Avec le modèle à vérification systématique, vous bénéficiez d'une meilleure visibilité sur vos utilisateurs, appareils, conteneurs, réseaux et applications, car vous vérifiez leur état de sécurité à chaque demande d'accès. Un n'exclut pas l'autre. Il est tout aussi important de s'assurer que les utilisateurs et les appareils qui accèdent aux applications répondent à vos exigences en matière de sécurité.

Pourquoi est-ce ambitieux?

Lorsque la plupart de notre personnel travaillait à distance, il était difficile pour les utilisateurs de savoir comment accéder aux différentes applications. Par exemple, certaines applications nécessitaient un RPV, tandis que l'on pouvait accéder à d'autres directement, ce qui causait beaucoup de frustration pour nos utilisateurs.

Historiquement, les entreprises ne passent pas beaucoup de temps à s'inquiéter des applications qui nécessitent une connexion au RPV par rapport à celles qui n'en ont pas besoin. Nous savons que les responsables des TI assument une partie de ce fardeau : ils doivent gérer des ordinateurs portables et des RPV pour un personnel qui est de plus en plus à distance. À l'instar de nombreuses autres entreprises, Cisco a investi dans l'expansion du RPV afin de soutenir le personnel travaillant à domicile. Dans la région de l'Asie-Pacifique, du Japon et de la Chine, nous avons élargi la capacité, y compris la bande passante et les groupes d'adresses IP. En Europe, au Moyen-Orient et en Afrique, nous avons constaté que notre capacité générale était bonne, mais que sa résilience devait être renforcée. En Amérique, nous avons augmenté les ressources de notre campus de San Jose et du Research Triangle Park, en Caroline du Nord. Nous avons également apporté les modifications nécessaires à nos points d'accès au RPV pour rediriger automatiquement et distribuer mondialement le trafic selon les besoins.

Cependant, il y a d'autres facteurs dont nous devons tenir compte pour un personnel flexible. La frontière entre le travail et la vie personnelle s'estompe pour de nombreuses personnes. Les membres de la famille peuvent partager des ordinateurs pour de petites tâches, y compris les travaux scolaires. Il est également normal de s'attendre à ce que les gens souhaitent séparer leur navigation personnelle et leur travail du RPV de l'entreprise. Il peut être frustrant d'activer et de désactiver le RPV à répétition. En outre, l'utilisation d'un RPV lorsque le personnel est presque entièrement à distance peut s'avérer inefficace, en particulier lorsque nous renvoyons des données sur le réseau de l'entreprise pour finalement devoir retourner dans le nuage. Il peut également être contrariant pour les utilisateurs de savoir quelles applications ont besoin d'un RPV et lesquelles n'en ont pas, ce qui a finalement une incidence négative sur leur productivité.

Ce fut le début de la transformation de notre façon de travailler. De nos jours, nous entendons parler de vérification systématique partout, et cela signifie vraiment quelque chose de différent pour tout le monde. Chez Cisco, nous nous sommes investis dans l'application des principes de la vérification systématique dans l'ensemble de l'entreprise et dans toutes les facettes de nos processus d'infrastructure.

Pour permettre cette nouvelle façon de travailler, nous avions besoin d'une nouvelle approche. Nous avons décidé d'appliquer les principes de la vérification systématique dans l'ensemble de l'entreprise afin que les utilisateurs puissent travailler n'importe où, à partir de n'importe quel appareil, et ce, en toute sécurité et sans friction.

Le plan

Obtenir l'adhésion

La première étape des services informatiques de Cisco a été d'élaborer un plan pour obtenir l'adhésion des cadres. Une erreur courante que nous avons constatée avec d'autres initiatives était que leur grande complexité les rendait difficiles à comprendre et à parrainer. Notre objectif était de rendre le message simple, précis et limité dans le temps, afin qu'il soit mémorable et facile à répéter aux autres.

Lorsque nous avons lancé le programme et rencontré nos cadres responsables, nous nous sommes concentrés sur trois avantages clés :

1. **Expérience d'authentification améliorée :** Nous avons souvent entendu les utilisateurs dire « J'ai l'impression de m'authentifier tout le temps. » Nous avons tenté de répondre à cette préoccupation en deux volets, en permettant une expérience moins dépendante des mots de passe et en commençant à appliquer les principes de la vérification systématique aux cas d'utilisation d'accès à distance, en supprimant la fiabilité implicite accordée par le périmètre traditionnel.
2. **Accès aux applications sans frontières :** Nous savons que vous ne pouvez pas considérer comme implicitement fiable un utilisateur simplement parce qu'il est sur le réseau. De la même manière, si nous sommes en mesure d'établir la fiabilité, nous pouvons autoriser l'accès à certaines de ces applications ou ressources pour lesquelles vous avez traditionnellement besoin d'un accès au RPV. Ce faisant, vous offrez une expérience plus transparente aux utilisateurs qui accèdent à ces applications sans avoir à savoir s'ils se trouvent sur un RPV, sur le réseau de l'entreprise ou ailleurs.
3. **Sécurité accrue :** L'accès n'est pas seulement axé sur l'utilisateur et sur la question de savoir si nous le considérons comme fiable, car il fournit son nom d'utilisateur et son mot de passe. Nous sommes également en mesure de demander : « Le terminal d'où il provient respecte-t-il une certaine posture de sécurité? Est-ce que son intégrité est intacte? » Duo nous offre une sécurité et une visibilité accrues pour restreindre l'accès en fonction de ce niveau de contexte.

Défis

- Protéger l'accès dans le monde entier
- Élargir l'accès aux utilisateurs en toute sécurité
- Sécuriser tous les utilisateurs et les appareils
- Offrir une expérience uniforme pour les utilisateurs

Solutions

- L'authentification multifactorielle (AMF) empêche les tentatives de connexion frauduleuses
- Trusted Endpoints limite l'accès aux appareils gérés
- Trust Monitor détecte les tentatives de connexion anormales
- L'application Duo Device Health garantit la sécurité des appareils
- Les politiques d'accès adaptatives bloquent les tentatives de connexion à risque
- Duo SSO simplifie l'accès avec un seul nom d'utilisateur et un seul mot de passe
- Duo Network Gateway offre un accès sans RPV

Résultats

- Plus de 100 000 utilisateurs et plus de 170 000 appareils sécurisés
- Déploiement en 5 mois
- Moins de 1 % des utilisateurs ont contacté le centre d'assistance
- 5,76 millions de contrôles d'intégrité par mois
- 86 000 appareils corrigés par mois
- 410 000 authentifications de moins par mois via DNG (sans RPV)

Les cadres responsables faisaient les choses très différemment que dans le passé. Au lieu d'attendre que le projet soit entièrement planifié avant de le partager, les parties prenantes étaient invitées à participer dès le début. Le projet a été parrainé par plusieurs cadres de la sécurité et des TI qui ont pu obtenir l'adhésion à leur niveau. Ils ont également fourni une protection au cas où l'équipe devait agir rapidement et casser des choses par inadvertance. Bien que la vitesse ait été jugée plus importante que la perfection, tout s'est déroulé comme prévu.

L'équipe de base était composée d'une personne représentant un pouvoir décisionnel :

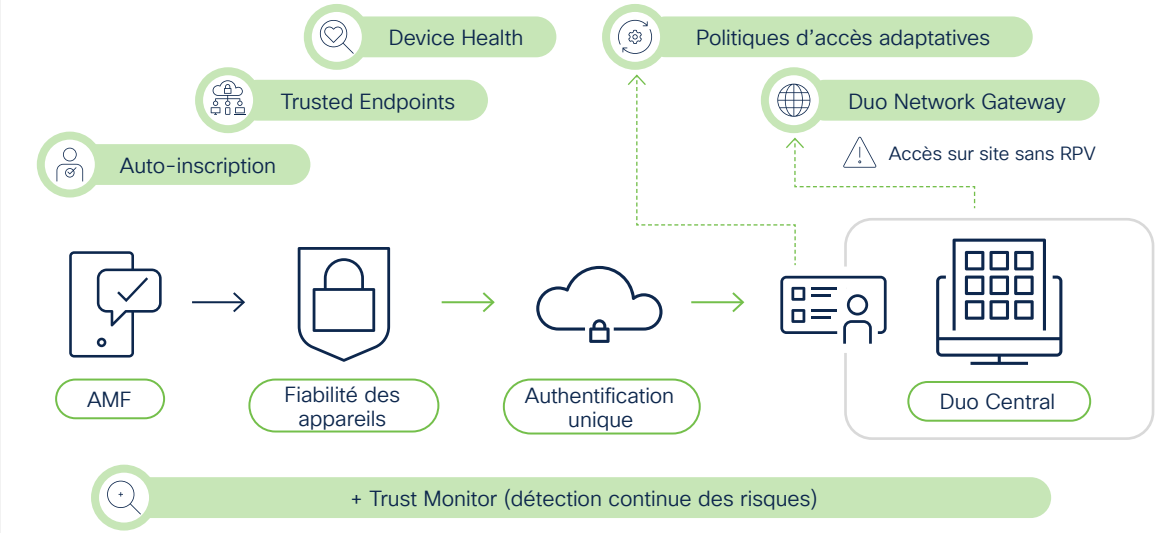
- Infrastructure
- Terminal
- Identité
- Suivi des applications
- Communications
- Sécurité de l'information

Équipe de base

L'équipe derrière cette vaste transformation était plus qu'un service ou un groupe de travail. Compte tenu des calendriers serrés, nous avons décidé dès le début que nous aurions une petite équipe de base pour diriger l'initiative avec quelqu'un pour représenter chaque fonction. Ce puissant petit groupe de spécialistes en ingénierie et en architecture a eu une grande influence sur la façon dont nous avons progressé. Ils ont été chargés de retourner auprès de leur organisation respective et de partager des informations, de solliciter des commentaires ou de demander d'aller de l'avant avec les différentes décisions prises. Les cadres responsables ont fourni des renforts et ont permis de surmonter les obstacles au besoin.

Le fait de prendre dès le début le temps de planifier la portée du projet, de mesurer et d'affirmer les jalons en cours de route, et d'identifier les membres de l'équipe de base a considérablement aidé. Le fait de disposer de plusieurs équipes spécialisées nous a permis de diviser le déploiement en plusieurs flux de travail, chaque fonction étant libre de se concentrer sur ses tâches. Des réunions hebdomadaires ont été organisées pour partager des mises à jour, avec une personne de chaque flux de travail, ce qui a permis à l'équipe de rester petite et efficace.

Objectifs techniques



D'un point de vue technique, notre objectif principal était de mettre en œuvre une architecture qui permettrait un accès sécurisé et sans RPV à certaines de nos applications internes et logiciels-services (SaaS) les plus visitées. Deuxièmement, nous voulions valider la fiabilité des utilisateurs et des appareils, en procédant par application, avec la possibilité de définir des politiques d'accès par application. Troisièmement, nous avons cherché à améliorer notre expérience d'authentification en réduisant le fardeau des utilisateurs. Enfin, nous voulions créer cette transition de manière transparente, sans aucune intervention de la part de l'utilisateur et sans interruption ni distraction. L'idée centrale derrière la vérification systématique est de valider la fiabilité des utilisateurs et des appareils à chaque accès à une ressource, plutôt que de considérer comme implicitement fiable l'appareil simplement parce qu'il est connecté à votre réseau d'entreprise. Qu'est-ce que cela signifie réellement?

Tout d'abord, nous avons besoin d'un moyen de vérifier la fiabilité des utilisateurs. Historiquement, on y arrivait avec une combinaison de nom d'utilisateur et de mot de passe, et plus récemment avec un deuxième facteur d'authentification. Si vous vous souvenez bien, l'un de nos objectifs avec ce programme était de réduire les frictions pour les utilisateurs en matière d'authentification.

Pour y parvenir, nous avons tiré parti d'un certificat d'identité utilisateur déployé en toute sécurité sur nos terminaux gérés par notre suite de gestion des appareils. Ce certificat agit ensuite comme premier facteur d'authentification, épargnant à l'utilisateur l'étape de devoir saisir son nom d'utilisateur et son mot de passe. Cette mesure réduit également la probabilité qu'un utilisateur enregistre simplement son identité d'entreprise et son mot de passe dans son navigateur Web pour plus de commodité. Nous voulons décourager ce comportement pour empêcher les tiers d'obtenir l'accès à nos informations d'identification d'utilisateur. De plus, en utilisant moins souvent le formulaire de nom d'utilisateur et de mot de passe, les utilisateurs deviennent indirectement plus vigilants contre l'hameçonnage. Ensuite, l'utilisateur satisfait un deuxième facteur d'authentification. Pour la plupart des utilisateurs, cela signifie accuser réception d'une notification poussée envoyée à leur téléphone sur l'application Duo Mobile.

Après avoir établi la fiabilité des utilisateurs, nous avons besoin d'un moyen de valider la fiabilité et l'intégrité des appareils. Il s'agit d'un nouveau domaine que le modèle d'architecture à vérification systématique vise à aborder. Chez Cisco, nous partons du principe que si un appareil est géré par nos plateformes de gestion des appareils d'entreprise, il doit avoir une bonne posture de sécurité de base. Cela comprend des garanties comme les derniers correctifs logiciels, l'écran verrouillé, le pare-feu et le chiffrement activé. Par conséquent, pour identifier un appareil fiable dans notre cadre à vérification systématique, nous utilisons des certificats d'appareil qui sont envoyés à chaque terminal par notre plateforme de gestion des appareils.

Enfin, nous allons encore plus loin pour vérifier la fiabilité des appareils. Bien que l'appareil ait peut-être été géré à un moment donné lors du déploiement du certificat de l'appareil, il est possible qu'un utilisateur particulièrement averti en technologie, ce que nous avons beaucoup chez Cisco, ait désactivé certaines des protections appliquées par notre plateforme de gestion. Pour atténuer ce problème, nous effectuons une vérification supplémentaire de l'intégrité de l'appareil lors de chaque transaction d'authentification pour nous assurer que l'appareil dispose toujours des derniers logiciels, de l'écran verrouillé, du chiffrement des lecteurs, du pare-feu et de l'agent antivirus en cours d'exécution. Cette vérification de l'intégrité en temps réel est effectuée par l'application Duo Device Health, qui fonctionne en arrière-plan en permanence sur l'appareil.

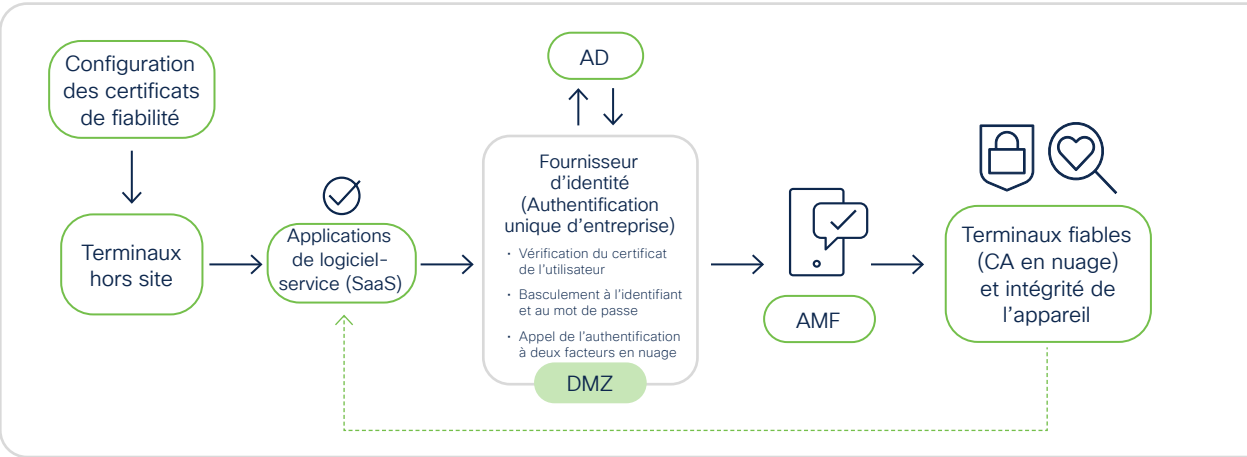
En résumé, lorsqu'un utilisateur tente de se connecter à une application, notre moteur d'authentification unique d'entreprise vérifie le certificat de l'utilisateur et de l'appareil, effectue une évaluation en temps réel de l'intégrité de l'appareil et déclenche finalement une notification de deuxième facteur avant d'autoriser l'accès de l'utilisateur. Nous le faisons, que l'application soit sur site, derrière le pare-feu de l'entreprise ou qu'il s'agisse d'une application de logiciel-service (SaaS). Maintenant que nous avons vu les éléments de haut niveau de cette architecture, examinons de plus près notre architecture de bout en bout.

Architecture à vérification systématique

Configuration

Le premier élément de cette architecture consiste à configurer correctement les terminaux. Nous avons un parc de plus de 170 000 terminaux, qui comprend une répartition presque égale de systèmes Mac et Windows, et plus de 60 000 terminaux de classe mobile, dont la plupart sont iOS, mais aussi un nombre important d'utilisateurs Android. Nous avons tiré parti de nos plateformes de gestion des appareils pour déployer les certificats de fiabilité des utilisateurs et des appareils sur les terminaux. Nous avons également déployé l'application Device Health sur les postes de travail des utilisateurs. Enfin, nous avons déployé des configurations pour les principaux types de navigateurs afin de sélectionner automatiquement le bon certificat, plutôt que d'inviter l'utilisateur à faire un choix. Nous utilisons Jamf pour gérer notre parc de Mac, SCCM et Intune pour gérer nos systèmes Windows, et Cisco Meraki pour gérer nos terminaux mobiles.

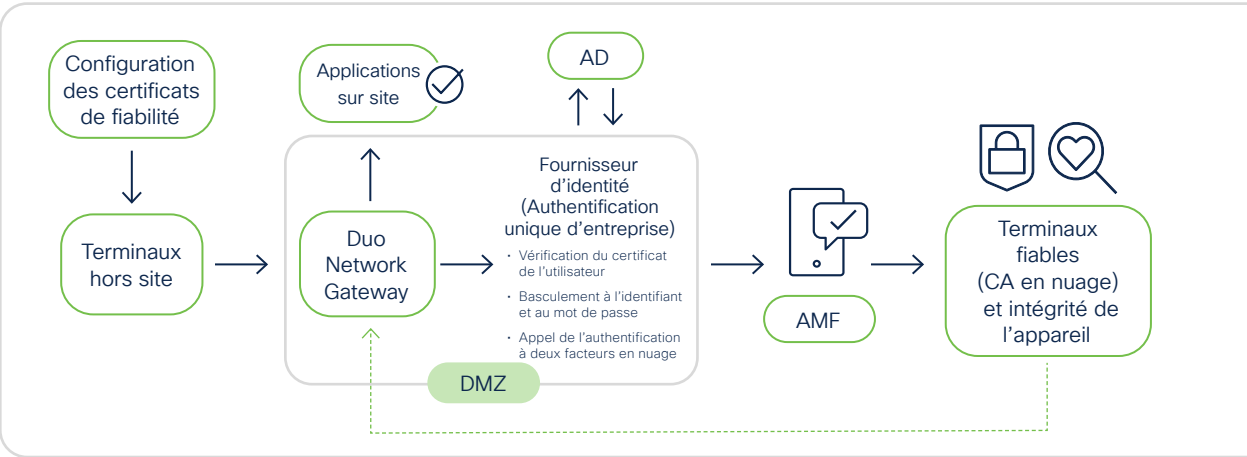
Applications de logiciel-service (SaaS)



L'architecture des applications de logiciel-service (SaaS) commence lorsque le terminal demande l'accès à une application Web en nuage. Cette demande lance une prise de contact SAML avec le fournisseur d'identité. Notre fournisseur d'identité tente de récupérer le certificat d'identité de l'utilisateur à partir du terminal et, lors de la réception d'un certificat valide, il vérifie que l'utilisateur est toujours un membre du personnel actif en recherchant ses informations dans Active Directory. Une fois toutes ces vérifications terminées, on invite l'utilisateur à satisfaire un deuxième facteur d'authentification, généralement au moyen d'une notification poussée de l'application Duo Mobile. Nous prenons également en charge d'autres méthodes d'authentification comme TouchID et YubiKeys.

Après avoir vérifié l'identité de l'utilisateur, nous procédons à la validation de la fiabilité de l'appareil. Cette validation commence par Duo qui interroge l'appareil pour un certificat de fiabilité d'appareil afin de confirmer qu'il appartient au même utilisateur. Après la validation du certificat, Duo appelle l'application Device Health en cours d'exécution sur le terminal, qui fournit son état d'intégrité en temps réel. Si aucun problème n'est signalé, le flux d'authentification est terminé et une assertion SAML est émise par notre fournisseur d'identité pour l'application de logiciel-service (SaaS). Si un appareil n'est pas conforme, l'application indique à l'utilisateur comment effectuer la mise à jour et résoudre le problème. L'utilisateur est alors autorisé à accéder à l'application.

Sur site

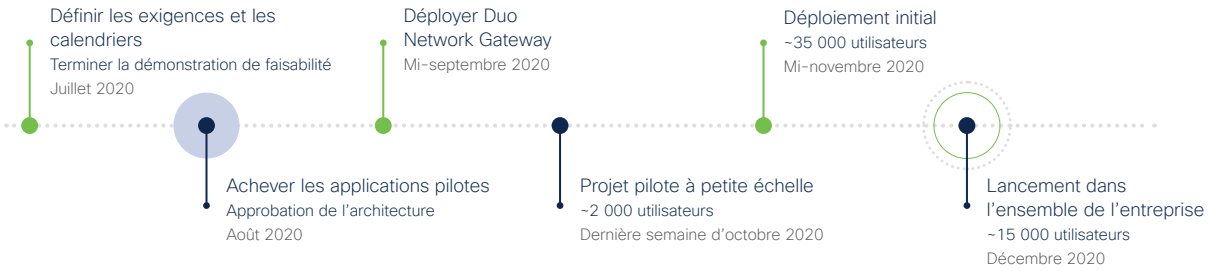


Le flux diffère légèrement pour les utilisateurs qui accèdent à une application sur site. Un élément clé qui rend le tout possible est Duo Network Gateway, un serveur mandataire inverse qui agit comme point de contrôle principal pour permettre un accès sans RPV. Lorsqu'un utilisateur tente de demander l'accès une application sur site dans son navigateur (par exemple, notre site Web intranet), la première chose qui se produit est que nos serveurs DNS renvoient l'adresse IP du serveur mandataire inverse au lieu de l'hôte réel de l'application. Ce mécanisme est communément appelé DNS fractionné.

Une fois que le navigateur est redirigé vers la passerelle réseau, il lance le même flux d'authentification décrit précédemment pour les applications de logiciel-service (SaaS). L'identité de l'utilisateur est d'abord validée, puis la fiabilité de l'appareil est vérifiée. Si les deux réussissent, les témoins de session pertinents sont émis et le navigateur de l'utilisateur est envoyé par serveur mandataire à l'application.

Calendrier

Comme susmentionné, il s'agissait d'un programme de cinq mois avec des objectifs, des engagements et des échéanciers clairement définis.



Mois 1 (juillet-août)

Nous avons consacré le premier mois à la réalisation de démonstrations de faisabilité avec des applications fictives. C'était la première fois que nous testions l'ensemble de l'architecture de bout en bout sur toutes nos plateformes d'appareils.

L'un des enseignements de cet exercice est qu'il est plus difficile que vous ne le pensez d'obtenir un comportement de navigateur cohérent sur quatre plateformes de système d'exploitation différentes. Même si les configurations du navigateur pour la sélection automatique des certificats étaient bien documentées, nous avons trouvé de nombreux cas limites, en particulier du côté de Windows, où nos politiques étaient en conflit avec d'autres politiques de groupe de l'entreprise et où la collecte et la sélection des certificats ne fonctionnaient pas toujours comme prévu. En fait, on peut affirmer sans risque de se tromper que le déploiement des certificats sur les terminaux, puis la collecte systématique de ces certificats par notre moteur d'identité, ont nécessité le plus grand nombre d'itérations avant de le faire fonctionner comme nous le souhaitions.

Au cours de cette période, nous avons également examiné nos journaux d'accès Web et de RPV sur plusieurs systèmes pour déterminer empiriquement nos applications Web les plus utilisées, à la fois de logiciel-service (SaaS) et sur site. Cette étape était importante, car elle nous a permis de nous concentrer sur les grandes victoires au lieu d'essayer de faire l'impossible. Nous avons réduit notre liste d'applications à environ 20, puis nous avons commencé à interagir avec les équipes d'application. Dans certains cas, nous avons dû effectuer un audit de sécurité de l'application sélectionnée pour nous assurer qu'elle répondait à toutes nos normes de sécurité d'entreprise avant de la rendre disponible pour un accès à distance.

Ce premier mois a également été celui où nous devions obtenir l'adhésion sur l'architecture. Cette étape nécessitait l'approbation de nos équipes de sécurité de l'information, des terminaux et de l'infrastructure. Une fois cette étape terminée, nous avons commencé à préparer notre infrastructure de production.

Mois 2 (septembre)

La prochaine grande étape a été notre déploiement de produits de Duo Network Gateway, une condition préalable pour rendre les applications sur site disponibles grâce à un accès à distance. Après cette étape, l'ensemble de la configuration était officieusement en direct. Tout appareil doté du certificat et de la fiabilité appropriés pourrait accéder aux applications sur site incluses sans avoir à utiliser le RPV.

Mois 3 et 4 (octobre-novembre)

Nous avons commencé par un projet pilote à petite échelle portant sur environ 2 000 utilisateurs au sein de notre organisation informatique. Cela signifiait le déploiement des configurations de terminaux et des certificats de fiabilité auprès de ce groupe et leur demande d'essayer les flux d'authentification sur site et de logiciel-service (SaaS). Les commentaires ont été pour la plupart positifs, ce qui nous a permis d'aller de l'avant dans les délais avec la portée de notre première vague de programmes prévue d'environ 35 000 utilisateurs répartis dans quatre organisations différentes au sein de Cisco.

Mois 5 (décembre)

Le temps investi lors de notre démonstration de faisabilité et de notre phase pilote a vraiment été rentable. Notre déploiement initial auprès de 35 000 utilisateurs a été une telle réussite que nous avons procédé à un déploiement complet en entreprise deux mois plus tôt que prévu. Depuis lors, nous avons continué à intégrer plus d'applications au programme de vérification systématique, et nos utilisateurs l'adorent.

Leçons apprises et pratiques exemplaires

Approche d'équipe

Une équipe de base composée d'une personne représentant chaque flux de travail a été habilitée à prendre des décisions pour leur organisation. L'équipe de base s'est réunie régulièrement pour des mises à jour, ce qui a permis aux gens de rester concentrés sur ce qu'ils devaient faire et d'être agiles dans la prise de décision. Il y a eu des moments dans le projet où nous avons dû nous écarter de l'échéancier du projet et retarder ou accélérer certains efforts, mais en ayant une équipe réduite, nous avons pu nous mettre d'accord sur les ajustements rapidement et efficacement.

Cadres responsables

Notre directrice des systèmes d'information et notre directeur de la sécurité et de la fiabilité ont offert leur plein soutien pour aller de l'avant avec notre initiative de vérification systématique. Notre projet de transformation a nécessité des efforts dans les domaines des TI et de la sécurité. En s'assurant d'avoir l'aval de nos cadres, notre équipe a été habilitée à prendre des décisions et à agir rapidement. Il ne faisait aucun doute qu'il s'agissait d'une initiative importante dans l'ensemble de l'organisation, et le soutien de la direction a contribué en faire une priorité.

Un projet pilote comme preuve

Un déploiement progressif a permis de garder la vérification systématique à la fois prioritaire et gérable. Plutôt que d'effectuer un déploiement sur toutes les applications et tous les utilisateurs à la fois, l'équipe a commencé avec un sous-ensemble d'applications et de services. Ce déploiement a permis de vérifier le processus, de cerner les problèmes et de les résoudre. Par conséquent, le déploiement complet a pu être lancé des mois avant la date prévue.

Notre approche continue d'introduire progressivement les principes de la vérification systématique dans l'ensemble de l'entreprise. Au lieu d'apporter des changements importants qui auront des conséquences sur la productivité et généreront du chaos, nous avons introduit la vérification systématique pour le personnel, mais nous nous sommes concentrés sur le scénario de télétravail, en offrant une nouvelle méthode d'accès sans frontières.

Créer une demande pour la vérification systématique

Nous avons adopté une approche méthodique pour introduire les principes de la vérification systématique dans l'ensemble de notre organisation. L'équipe a commencé par permettre à tous les utilisateurs d'utiliser la technologie de Duo, puis a ajouté des applications à l'architecture à vérification systématique au fil du temps. Cette démarche a contribué à créer une demande pour le programme et a facilité le processus pour les utilisateurs. Pour faciliter la hiérarchisation, nous avons invité les utilisateurs à proposer des applications à inclure dans le programme. De plus, nous avons mis au point un processus permettant aux propriétaires d'applications de demander l'application de la vérification systématique pour leurs applications.

Lors de nos rencontres avec notre personnel, nous avons souligné qu'il s'agissait essentiellement d'une initiative visant à améliorer la posture de sécurité globale de Cisco. Nous leur avons également expliqué que l'expérience leur serait bénéfique en fournissant un accès sécurisé sans friction si leur appareil avait été validé comme étant géré et que son intégrité est intacte. Il est rarement possible d'améliorer l'expérience utilisateur tout en augmentant la sécurité. Nous croyons qu'en appliquant les principes de la vérification systématique, vous pouvez y parvenir.

Transparence totale et communication régulière

Nous ne saurions trop insister sur l'importance de communiquer activement avec vos parties prenantes, votre direction et votre personnel. Nous disposions de plusieurs canaux pour tenir les gens au courant. Un bulletin hebdomadaire de mises à jour a été envoyé à toutes les personnes qui s'y inscrivaient, un site SharePoint a été créé pour expliquer ce qui se passait, des forums étaient disponibles pour les commentaires du public ainsi que des courriels, des articles et des conseils pour la communication avec la direction.

Une fois que nous nous sommes mis d'accord sur le moment de lancer notre projet, nous avons décidé d'envoyer à nos parties prenantes, à la haute direction et aux parties intéressées un bulletin hebdomadaire qui montrait bien en évidence le nombre de jours restants avant la date de lancement de notre projet. Ayant plusieurs objectifs, le bulletin comportait les réalisations de cette semaine et les problèmes en suspens. Tout d'abord, elle a responsabilisé nos équipes. Nous avons ressenti un sentiment d'urgence pour nous assurer de garder le feu vert pour le projet. Ensuite, cela nous a donné une plateforme unique pour informer les parties prenantes des défis et des problèmes. Après avoir partagé les défis d'une semaine donnée, il était assez courant qu'un membre de la direction demande comment il pourrait aider à résoudre les obstacles auxquels nous étions confrontés.

L'engagement auprès de notre personnel était également très important. Bien que vous puissiez essayer d'offrir la meilleure expérience à votre personnel, la réalité est que vous aurez une incidence négative sur eux, ou du moins sur certains utilisateurs, en cours de route. Nous avons créé plusieurs forums, comme notre site SharePoint et notre alias d'équipe, où nos utilisateurs peuvent formuler leurs commentaires. Nous avons également rencontré notre organisation de soutien sur une base hebdomadaire pour mieux comprendre s'il y a des domaines que nous devons aborder, qu'il s'agisse de la documentation de l'utilisateur final, des possibilités de formation en matière d'assistance ou simplement de la sensibilisation aux nouveaux problèmes.

Cisco aujourd'hui

Déploiement

- Nous avons déployé des configurations de Duo sur plus de 180 000 terminaux, y compris l'ensemble de notre parc d'appareils iOS, Android, Mac et Windows gérés par les services informatiques de Cisco. Ce nombre continue de croître, car tous les appareils nouvellement inscrits reçoivent automatiquement les configurations nécessaires.
- Nous avons introduit cette nouvelle méthode d'accès sans frontières pour plus de 120 applications clés de l'entreprise. Depuis l'annonce de la disponibilité de l'accès sans frontières, nous avons reçu un nombre incroyable de demandes pour l'activer pour d'autres applications.
- Nous nous sommes engagés auprès des propriétaires d'applications sur la façon dont leurs utilisateurs peuvent tirer parti de cette nouvelle méthode d'accès en leur fournissant une liste documentée des exigences, en leur permettant d'effectuer des tests dans des environnements de préparation et en leur offrant le formulaire à utiliser pour poser des questions.

L'avenir de la vérification systématique chez Cisco

Depuis l'intégration des contrôles de l'intégrité et de la fiabilité des appareils au niveau de la couche applicative, notre capacité à réagir aux risques liés aux appareils s'est considérablement améliorée. Par exemple, environ 5,76 millions de vérifications de l'intégrité des appareils sont effectuées automatiquement chaque mois. Cela s'est traduit par la découverte de 86 000 appareils en un mois que les utilisateurs ont corrigés eux-mêmes. C'est 86 000 compromissions potentielles évitées sans effort.

Bien que l'augmentation du volume d'appels d'assistance ait suscité certaines inquiétudes lors de l'introduction des vérifications de l'intégrité des appareils pour l'accès sans frontières, nous avons constaté que moins de 1 % de nos utilisateurs ont communiqué avec le service d'assistance pour obtenir de l'aide. Nous estimons que les étapes de correction faciles à suivre dans l'application Duo Device Health ont joué un rôle clé dans la réduction du nombre de demandes de soutien.

Bien que nous ayons fait des progrès importants en peu de temps, notre équipe s'est rendu compte qu'il y avait beaucoup plus à faire dans notre parcours vers la vérification systématique. Nous prévoyons déjà des domaines à développer, comme la simplification du processus d'intégration des applications. Ces processus comprennent la validation de la satisfaction des exigences de connexion d'une application et les modifications nécessaires aux listes de contrôle d'accès et aux configurations de Duo Network Gateway. L'automatisation nous permet d'accélérer le processus d'intégration des applications et de réduire les erreurs humaines. Enfin, nous prévoyons d'intégrer la prochaine solution sans mot de passe de Duo et de simplifier et de sécuriser davantage l'expérience de l'utilisateur. Les services informatiques de Cisco se concentrent également sur l'élargissement de l'utilisation de la vérification systématique au-delà de l'écosystème immédiat de Cisco pour utiliser des scénarios tels que le paysage des partenaires extranet et l'intégration des acquisitions de manière plus transparente et moins gourmande en infrastructure.