Question : Les vpn font du 802.1X ? - Xavier C. (min.14)

Réponse (Pascal D.) : Non, seulement sans-fil et filaire. Mais d'autres mécanismes existent en VPN pour abourtir au même résultat. 802.1X est un protocole Layer 2, pas compatible avec du VPN.

Question : Je n'ai pas bien compris cette partie. - Patrick T. (min.25)

Réponse (Pascal D.) : Ce n'est pas simple de comprendre les différences entre AD on-prem & Azure AD. Mais c'est important pour ne pas souhaiter des scénarios impossibles ...

Question : Est-ce que le NAC (802.1x) est supporté pour Cisco ip phones enregistré dans un call manager express ? - Percy M. (min.29)

Réponse (Pascal D.) : Oui.

Question : ISE peut-il voir que 2 MAC identiques sont actifs en même temps ? - Davi F. (min.30)

Réponse (Pascal D.) : Ce scénario est possible et soit légitime, soit non. Légitime, le user change de port. Illégitime, les deux sont actifs en même temps. Deux choses, la MAC (en cas de MAB) est un identifiant unique d'asset. La dernière information est la bonne. On peut aussi activer (dans le cas de Profiling) le "Anomalie Behavior" qui générera des alarmes en cas d'anomalie.

Question : Je n'ai pas bien compris la partie SGT - Noubibom A. (min.42)

Réponse (Pascal D.) : https://gblogs.cisco.com/fr/reseaux/do-you-trustsec-la-securite-contextuelle-meme-en-wi-fi/#:~:text=Cisco%20propose%20une%20architecture%20de,de%20l'adressage%20IP%20des

Réponse (Jérôme D.) : Un SGT est un attribut donné par le serveur Radius lors de l'autorisation. C'est un groupe de sécurité qui est indépendant du VLAN et de l'adresse IP. Il est ensuite possible de faire des règles de sécurité avec ce tag. Ça permet d'avoir une sécurité non dépendante de la topologie réseau et aussi de faire de la microsegmentation.

Question : Où peut-on trouver la liste des FW Ngen compatible SGT ? - Davi F. (min.43)

Réponse (Pascal D.) : https://www.cisco.com/go/csta C'est une url avec toutes les possibilités d'intégrations. Avec un peu de recherche, on peut sélectionner les FW uniquement.

Question : Le firewall peut être d'une autre marque ? - Pierre-Arnauld L. (min.44)

Réponse (Pascal D.) : Oui, s'il est compatible, ce qui est le cas de la majorité des marques.

Question : A-t-on une liste officielle des compatibilités des autres constructeurs ? Pour une auth chaining EAP-FAST - Jérémy K. (min.45)

Réponse (Federico Z.) : Bonjour Jérémy. EAP-Chaining / TEAP sont supportés avec le supplicant Cisco AnyConnect ou nativement avec Windows 10, comme évoqué par Christophe. ISE supporte ces méthodes EAP avec tout équipement réseau / NAD qui supporte du 802.1X : le NAD n'intervient pas dans le support/choix de la méthode EAP, qui ne dépend que du client et du serveur d'authentification.

Question : ISE supporte bien les dictionnaires des autres constructeurs ? - Stéphane T. (min.45)

Réponse (Pascal D.) : Les dictionnaires de l'ISE sont extensibles. Soit avec des extensions disponibles directement dans l'ISE, qu'il suffit d'activer. Il est aussi possible de créer vos propres extensions. Dans le cas d'un éditeur inconnu de Cisco.

Question : Qui descend les règles associées au SGT au NAD ? et à quel moment c'est fait ? - Mohand H. (min.52)

Réponse (Jérôme D.) : Ça peut faire l'objet d'un webinar dédié! Le serveur radius associe le SGT à la connexion. La règle de sécurité peut être configurée de différente manière: soit elles sont téléchargées par l'équipement depuis ISE en Radius, soit des règles configurées en local sur l'équipement (CLI/GUI). Un équipement réseau va télécharger les règles pour un SGT à partir du moment où il en a connaissance. Un équipement ne télécharge ainsi que les règles (ou SGACLs) utiles. Et ça permet d'être extrêmement efficaces en termes de gestion de ressources.

Question : Les SGACL sont-ils téléchargés uniquement sur le NAD sur lequel le device est connecté (avec le SGT du device et les ACL associés) ou sont-ils poussés sur tous les NAD ? - Mohand H. (min.57)

Réponse (Jérôme D.) : Non, une SGACL est téléchargée par tout équipement configuré pour Trustsec (c'est indépendant du NAD) qui a connaissance d'un SGT particulier. Si par exemple un switch connecte un device dans le SGT 5, alors il va télécharger toutes les SGACLs qui ont pour destination le SGT 5. Je précise que les SGACLs ne sont pas poussées, elles sont téléchargées.

Question : C'est quoi le rôle de stealthwatch dans DNAC trust Analytics ? - Mohand H. (min.69)

Réponse (Thomas M.) : Stealthwatch (Cisco Secure Analytics) n'intervient pas, il s'agit bien d'une fonctionnalité porté par DNAC.

Question : Est-ce qu'il y a un risque que de l'info potentiellement confidentielle soit envoyée sur le cloud pour le machine learning ? - Francois L. (min.76)

Réponse (Pascal D.) : Seul des metadatas sont envoyés dans le cloud. Aucune information personnelle n'est envoyée. Auncun contenu de payload.

Question : La notion de trust score est-elle (ou sera-t-elle) disponible sur le Dashboard Meraki pour une infra Meraki avec ISE ? - Anas G. (min.77)

Réponse (Thomas M.) : Le trust score n'est pas disponible aujourd'hui sur le dashboard Meraki.

Question : Comment faire de la posture sur du guest ou prestataire via vpn ? Temporal ? - Stéphane T. (min.83)

Réponse (Pascal D.) : On y est, le temporal agent et/ou Agentless. Mais plus limité, logique, la table résume les choses.

Question : agentless = credentials sur le poste à contrôler ? - Stéphane T. (min.89)

Réponse (Pascal D.) : L'agentless = agent au travers d'une session web, exécuté dans l'environnement du navigateur, seulement possible si session avec navigateur. Temporal Agent = Un mini AnyConnect, qui s'installe le temps de valider la posture et se désinstalle juste après. Différent usage, agentless -> guest, temporal -> partenaire un accès avec un PC non managé.

Question CHAT : Cette authentification est forcément liée au serveur Radius ? - Cheick D. (min.14)

Réponse (en attente) :

Question CHAT : Les Meraki ne sont pas pris en charge par le DNA? Il faut obligatoirement un Catalyst ? - Emmanuel (min.67)

Réponse (Thomas M.) : Effectivement, les équipements Meraki sont gérés uniquement depuis le dashboard Meraki et non pas depuis un DNA Center.