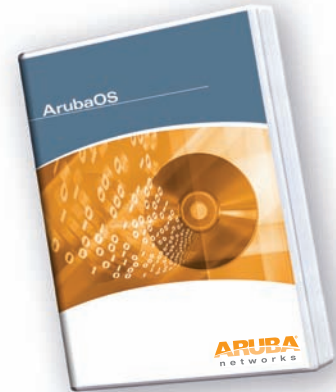




MODULE ARUBAOS D'APPLICATION DES STRATÉGIES DE PARE-FEU (PEF – POLICY ENFORCEMENT FIREWALL)

Le module d'application des stratégies de pare-feu Aruba (PEF) offre aux réseaux orientés utilisateur une sécurité basée sur l'identité, un contrôle de la qualité de service et des fonctions de gestion du trafic. La sécurité basée sur l'identité est fondamentale dans la mesure où les utilisateurs mobiles peuvent pénétrer dans un réseau à n'importe quel endroit, qu'il soit câblé ou non. Le pare-feu dynamique certifié ICASA d'Aruba permet la classification des utilisateurs en fonction de leur identité, du type d'appareil utilisé, de l'emplacement, de l'heure de la journée, et il fournit un accès différencié à des groupes d'utilisateurs distincts.



PARE-FEU DYNAMIQUE BASÉ SUR L'IDENTITÉ

- Les stratégies de pare-feu prennent en considération l'utilisateur, et pas uniquement les adresses IP, ce qui permet une plus grande visibilité et un contrôle plus exhaustif.

CERTIFICATION ICASA

- Permet l'application des règles de sécurité d'entreprise. La conformité à une règle de sécurité de l'entreprise devient obligatoire et est appliquée au lieu d'être simplement surveillée

CONTRÔLE D'ACCÈS BASÉ SUR LES STRATÉGIES

- Permet l'application des règles de sécurité d'entreprise. La conformité à une règle de sécurité de l'entreprise devient obligatoire et est appliquée au lieu d'être simplement surveillée

CONTRÔLE DE LA QUALITÉ DE SERVICE

- La classification dynamique des flux permet d'identifier les flux applicatifs pour un traitement spécifique, telle qu'une meilleure qualité de service pour les flux voix.

CONTRÔLE D'ACCÈS BASÉ SUR DES RÔLES

- Permet d'appliquer des modèles en fonction de l'appartenance à un groupe, ce qui simplifie l'administration

SÉCURITÉ HAUTES PERFORMANCES

- Chiffrement/déchiffrement accéléré au niveau matériel et traitement des stratégies de pare-feu pour éliminer les goulets d'étranglement
- Séparation du circuit de contrôle et du circuit de données pour plus d'évolutivité

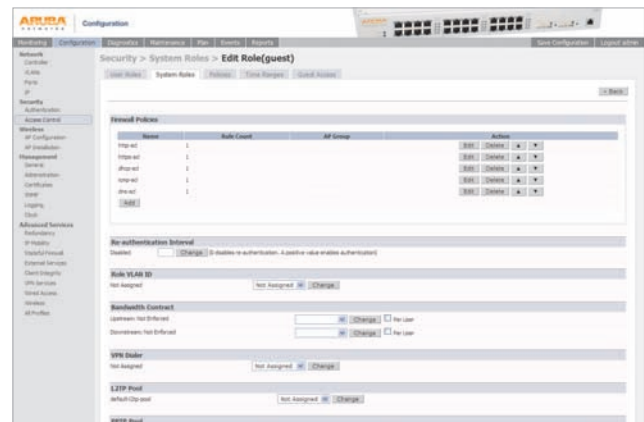
Étant donné que les réseaux mobiles ne disposent pas d'une couche physique de sécurité, les utilisateurs mobiles doivent être traités de manière plus sécurisée que les utilisateurs fixes traditionnels. Les pare-feu sont obligatoires dans la stratégie de sécurité en couche d'une entreprise pour le réseau mobile. Grâce à la technologie unique de pare-feu dynamique basée sur l'identité d'Aruba, les entreprises peuvent définir des contrôles d'accès pour tout utilisateur ou groupe d'utilisateurs du réseau.

PARE-FEU DYNAMIQUES BASÉS SUR L'IDENTITÉ

Les contrôleurs de mobilité Aruba fournissent un point unique de chiffrement/déchiffrement, d'authentification et d'application du pare-feu. Parce qu'ils tiennent compte de l'identité et terminent le chiffrement, ils protègent des attaques malicieuses dont pâtissent les pare-feu réseau traditionnels qui filtrent en fonction de l'adresse IP plutôt qu'en fonction de l'identité de l'utilisateur.

CONTRÔLE D'ACCÈS COMPLET BASÉ SUR LES STRATÉGIES DE PARE-FEU

Toutes les entreprises possèdent des règles de sécurité informatique écrites. Ces stratégies peuvent imposer l'accès réseau, les protocoles et applications autorisés ou refusés, ainsi que les niveaux de services fournis. Dans la plupart des entreprises, la conformité à ces stratégies est surveillée à des degrés divers, mais les infractions sont découvertes et réglées après avoir été commises. Aruba permet aux stratégies d'être appliquées activement, même dans un environnement mobile, et les stratégies suivent les utilisateurs lorsqu'ils se déplacent en périphérie de réseau.



Interface graphique simple à utiliser pour le centre de configuration des stratégies de pare-feu.

CONTRÔLE DE LA QUALITÉ DE SERVICE

Une fois les flux d'applications identifiés par le pare-feu, les opérations standard de pare-feu telles que l'autorisation, l'interdiction, la journalisation ou le rejet peuvent être appliquées. Cependant, la fonction de pare-feu dynamique d'Aruba offre plus qu'une sécurité puissante. Les actions des stratégies peuvent aussi étiqueter les paquets avec un indicateur 802.1p ou DSCP, classer le trafic par priorité en plusieurs files d'attente ou même rediriger des protocoles spécifiques vers diverses destinations. La classification des flux est dynamique pour plusieurs protocoles couramment utilisés, notamment le protocole SIP, ce qui permet d'appliquer une qualité de service appropriée au protocole de contrôle et aux sessions d'appels.

CONTRÔLE D'ACCÈS BASÉ SUR DES RÔLES

Le pare-feu d'application des stratégies dynamique d'Aruba permet d'accéder aux ressources réseau en fonction du rôle de l'utilisateur. Ce rôle est attribué ou provient de plusieurs mécanismes différents

MODULE ARUBA OS D'APPLICATION DES STRATÉGIES DE PARE-FEU (PEF – POLICY ENFORCEMENT FIREWALL)

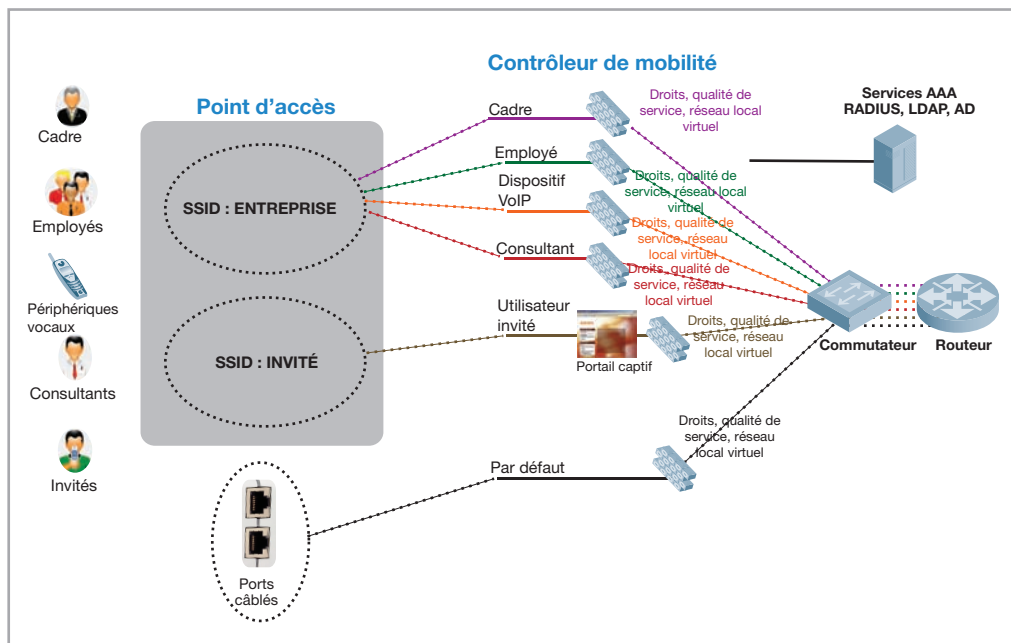
tels que les bases de données d'authentification externe, les ESSID ou l'emplacement physique. Une fois qu'un rôle a été attribué à un utilisateur, des stratégies différenciées peuvent être appliquées

SÉCURITÉ SANS FIL HAUTES PERFORMANCES

Jusqu'à maintenant, les entreprises étaient forcées de mettre les utilisateurs sans fil en quarantaine dans une zone démilitarisée où ils étaient authentifiés et passaient par le pare-feu comme s'ils provenaient d'Internet. Ce mécanisme fonctionne certes du point de vue de la sécurité, mais les performances offertes à l'utilisateur sans fil en sont énormément affectées en raison des limites liées aux pare-feu et aux passerelles VPN basées sur une zone démilitarisée. Aruba permet aux utilisateurs d'entreprise d'être authentifiés, chiffrés et de passer par le pare-feu au sein du réseau interne de l'entreprise, avec un niveau de sécurité et de performances élevé, fournissant ainsi le point de connexion entre les utilisateurs mobiles et le réseau câblé.

SPÉCIFICATIONS

- Certification
 - Corporate Firewall v4.1* certifié ICASA (*Aruba 6000 uniquement)
- Critères de détermination des rôles
 - Authentification – Par défaut ou basée sur RADIUS
 - Emplacement physique
- Passerelle applicative dynamique
 - Protocole FTP
 - Protocole SIP
 - Protocoles RTP/RTSP
 - Cisco SCCP (Skinny)
- Qualité de service avec et sans fil
 - Classification des flux
 - Files d'attente prioritaires
 - Contrats de bande passante
 - Étiquetage 802.1p et DSCP
- Traduction des adresses réseau
 - Source et destination



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tél. +1 408.227.4500 | Fax +1 408.227.4550