

 Rex0519 Update CR5.md Latest commit 7a4ddd 1 minute ago  History

 1 contributor

#CR5

ACLS AVANCÉES

1. ACL DYNAMIQUE

L'ACL dynamique refuse initialement le passage du paquet de données correspondant de l'utilisateur. Lorsque l'utilisateur est authentifié avec succès, les données sont temporairement libérées, mais une fois la session terminée, l'ACL est restaurée dans sa configuration d'origine. Pour définir le moment où l'ACL dynamique est restaurée dans la configuration d'origine, nous pouvons définir le délai d'expiration de la session, on sort s'il arrive le temps d'attente sans opération, ou nous pouvons aussi définir l'heure absolue, la session doit être déconnectée après l'heure spécifiée.

'access-list 100 dynamic ccie timeout 120 permit icmp any any' Pour les données qui peuvent passer après l'authentification, telles que ICMP, le temps absolu est de 2 minutes.

!!!attention: login local pour les lignes est obligatoire.

2. ACL RÉFLEXIVE

Cette ACL est intéressant pour moi. ça a l'air comme un ESTABLISHED avancé.

Le principe de fonctionnement est de juger le trafic de l'extérieur, s'il s'agit du trafic de retour du réseau interne, il peut être libéré, et s'il s'agit du trafic interne généré par une source externe, il est rejeté.

ACL RÉFLEXIVE enregistrera l'état de chaque connexion, puis libérera le trafic inverse légal basé sur l'enregistrement.

Cependant, l'ACL réfléchissant a ses limites.

Il ne peut rien faire pour les services avec des trafics aller et retour différentes (tels que FTP actif, NFS, etc).

Sinon, comment vendre le pare-feu?

'Router(config-ext-nacl)#permit ip any 192.168.2.0 0.0.0.255 reflect back_to_1 timeout 30 % Autorisez 192.168.1.0/24 à accéder à 192.168.2.0/24, et lorsque l'entrée correspond au trafic, ajoutez automatiquement une entrée autorisée inversée avec un délai d'expiration de 30 s à l'ACL réfléive nommée back_to_1'

'Router(config-ext-nacl)#evaluate back_to_1 % Mappez toutes les entrées de l'ACL réflexive nommée back_to_1 à cette ACL'

3. ACL BASÉ SUR TEMPS

Évidemment, l'ACL est déterminée en fonction du temps

'time-range a-name'

'periodic Monday ... h:mm to h:mm'

'access-list 101 permit udp IP MASK any dns time-range a-name'

Pare-feu

Il existe plusieurs avantages a utiliser un pare-feu dans un reseau:

- Empêcher l'exposition des hotes, des ressources et des applications sensibles aux utilisateurs non approuves.
- Inspecter le flux de protocole, ce qui empêche l'exploitation des failles de protocole. Bloquer les données malveillantes des serveurs et des clients.
- Réduire la complexité de la gestion de la sécurité en déchargeant la majeure partie du contrôle d'accès au réseau sur quelques pare-feu du réseau.

Attention Les pare-feu présentent également certaines limitations:


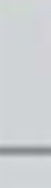


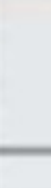













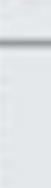



















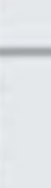
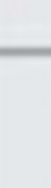




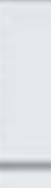




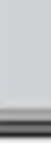












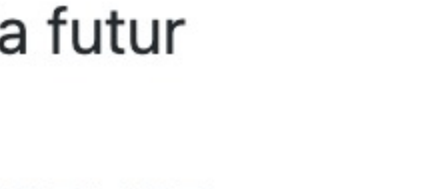






- Un pare-feu mal configuré peut avoir de graves conséquences pour le réseau, comme devenir un point de défaillance unique.
- Les données de nombreuses applications ne peuvent pas être transmises via les pare-feu en toute sécurité.
- Les utilisateurs peuvent rechercher de manière proactive des moyens de contourner le pare-feu pour recevoir du contenu bloqué, ce qui expose le réseau à une attaque potentielle.
- Les performances du réseau peuvent ralentir.
- Le trafic non autorisé peut être tunnelisé ou masqué en tant que trafic légitime à travers le pare-feu.

PARE-FEU DE NOUVELLE GENERATION

Un pare-feu de nouvelle génération va au-delà du pare-feu avec état de plusieurs manières importantes:

- Identification, visibilité et contrôle granulaires des comportements dans les applications
- Restreindre l'utilisation du Web et des applications Web en fonction de la réputation du site
- Protection proactive contre les menaces Internet
- Application des politiques en fonction de l'utilisateur, de l'appareil, du rôle, du type d'application et du profil de menace
- Performance de NAT, VPN et inspection de protocole avec état (SPI) Utilisation d'un système intégré de prévention des intrusions (IPS)

PARE-FEU DE NOUVELLE GÉNÉRATION

Top Next-Generation Firewall Vendors															
	Security Performance			Value			Implementation			Management			Support		
	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD
															
															
															
															
															
	Unable to evaluate														
	Unable to evaluate														
															
															
															

ZPF

a la futur

PFSENSE

LE FIREWALL PFSENSE

Le projet pfSense, est basé sur un fork de mOnOWall réalisé en 2004 par Chris Buechler et Scott Ullrich11.

pfSense est un routeur/ pare-feu open source basé sur le système d'exploitation FreeBSD.

À l'origine un fork de mOnOWall, il utilise le pare-feu états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires.

pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

installation

0. LAN segment dans conf de VMWARE Workstation
1. configuration des adresses IP pour WAN et LAN sur 1 et 2
2. configuration l'accès WAN

' pfSsh. php playback enableallowallwan'

configuration de chaque service

1. SSH
2. NAT
3. ALLIASES
4. VIRTUAL IPs
5. TRAFFIC SHAPER(limite débit)

outil (PLUGIN EXTRA)

- NTOPNG (outil d'analyse)
- PFBLOCKERNG protection de la vie privée et de traçage avec filtrage Web permettant d'améliorer la confidentialité, de contrôler les accès, de supprimer les publicités et de bloquer l'accès aux sites publicitaires.

MULTI-WAN pour plusieurs LSPs ou MSOs

1. la balance de la charge
2. l'Agrégation de liens

Redondance

- High Availability Sync PFSYNC
- Common Address Redundancy Protocol (CARP) open redundancy solution for sharing IP addresses among a group of network devices. Similar solutions already existed, primarily the IETF standard for Virtual Router Redundancy Protocol (VRRP). However Cisco claims VRRP is covered by its patent on their Hot Standby Router Protocol (HSRP), and told the OpenBSD developers that it would enforce its patent.

IDS ET IPS

A VENIR

some tricks

simulation un VPC par un routeur:

no ip route

ip default-gateway a.b.c.d

rewrwr