Activité : configurer un VPN IPsec

Présentation

Cette activité consiste à configurer un tunnel IPsec entre deux SNS Stormshield en utilisant :

- soit l'environnement virtuel mis en place avec VirtualBox en configurant le tunnel entre les agences A et B;
- soit l'environnement virtuel mis en place avec Proxmox en configurant le tunnel entre deux équipes .

La suite de ce document est réalisé dans l'environnement mis en place avec VirtualBox.

Définir la politique de filtrage

Réactiver la politique de filtrage (10) Pass All.

Configurer le tunnel IPsec avec une clé partagée sur le premier SNS

- Depuis l'interface d'administration du SNS de l'un des extrémités du tunnel, accédez au menu VPN ⇒ VPN IPsec > onglet POLITIQUE DE CHIFFREMENT - TUNNELS;
- Dans la rubrique SITE À SITE (GATEWAY GATEWAY), cliquez sur Ajouter ⇒ Tunnel site à site.

				1	Edit					
				0	Reset					
			/	Ŀ	Copy to	•				
O VPN / IPSEC	VPN									
	OLICY - TUNNE	LS	PEERS	IDENTIFICA	TION	ENCRYPTI	ON PROFILE	S		
4 IPsec 01 (01)	- ₹	Actions	•••••••••••••••••••••••••••••••••••••••							
SITE TO SITE (G	ATEWAY-GATE	WAY)	MOBILE -	MOBILEUS	ERS					
Q Enter a filter	*	- x *	+ Add -	× Delete	🕇 Up	I Down	🛛 🛃 Cut	🔁 Сору	🕑 Paste	Show details
🦺 (1) IPsec 01	Status	≞ v	Standard site	-to-site tunnel	e er		Remote net	work	Encryption	profile
(2) IPsec 02			Separator (ru	le grouping)						
(3) IPsec 03										
(4) IPsec 04										
(5) IPsec 05										
(6) IPsec 06										
(7) IPsec 07										
(8) IPsec 08										
(9) IPsec 09										
(10) IPsec 10										

- l'assistant de création du tunnel VPN IPsec permet de renseigner les principaux paramètres :
- les extrémités de trafic (objet réseaux local et objet réseau distant)
- l'extrémité de tunnel distante (le correspondant).



L'assistant de création du correspondant permet de renseigner les paramètres du correspondant :

 la passerelle distante en renseignant l'objet machine qui porte l'adresse IP du correspondant.

la clé partagée (PSK)

ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2		\approx
IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE C	RÉATION D'UN CORRESPONDANT IKEV2	
Certificat : Autorité de confiance (optionnel) : Clé prépartagée (ASCII) :	Certificat Certificat Certificat Autorité de confiance MotDePasseSecret	
Confirmer :	MotDePasseSecret	
	Saisir la clé en caractères ASCII X Annuler	

La dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours.
 Cliquez sur **Terminer**, on retourne sur l'assistant de création du tunnel VPN.

activiteipsec

ASSISTANT DE	SSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2					
RÉSUMÉ - ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2						
	Paramètres du site distant :					
	Nom :	Site_Fw_B				
	Passerelle distante :	Fw_B				
	Identification du correspon	dant : clé prépartagée				
	Clé prépartagée :	4d6f744465506173736553	6563726574			
						_
			× Annuler	≪ Précédent	 Terminer 	

• Sur la page de l'assistant de création du tunnel VPN, cliquez sur Terminer.

Le tunnel VPN IPsec est ajouté sur une ligne distincte de la politique.

Un résumé détaillé des paramètres de configuration peut être affiché en cliquant sur le pictogramme représentant un oeil.

Network Security	MONITORING CONFIGURATION EVA1 SNS_EVA1_V4_A				
★ - « © CONFIGURATION -	CO VPN / VPN IPSEC				
Rechercher * *	POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT				
₩ SYSTÈME	(1) IPsec 01 Activer cette politique Editer + 0				
néseau	SITE À SITE (GATEWAY-GATEWAY)				
S OBJETS	Texte recherché 🛛 😽 + Ajouter - 🗙 Supprimer 🗈 Monter 🖡 Descendre 🛛 🔀 Couper 🖄 Coller				
LUTILISATEURS	Ligne Etat Réseau local Correspondant Réseau distant Profil de chiffrement Keepalir				
+ POLITIQUE DE SÉCURITÉ	1 💽 on Vetwork_in Site_Fw_B Lan_in_B StrongEncryption 0				
PROTECTION APPLICATIVE	Résumé de la ligne 1 de la politique de chiffrement 1				
CO VPN	Version d'IKE :2				
VPN IPsec	Correspondants : Local: Tous (Any) Distant: Machine : 192.36.253.20 (Fw_B)				
VPN SSL Portail	Trafic chiffré : Local : Réseau : 192.168.1.0 / 255.255.255.0 (Network_in)				
VPN SSL	<u>Distant :</u> Réseau : 192.168.2.0 / 255.255.255.0 (Lan_in_B)				
Serveur PPTP 🕁	Paramètres d'authentification :				
NOTIFICATIONS	Mode : Type : psk Local ID : ID du correspondant : Clé prépartagée : 4d6f7444655061737365536563726574 Profil de chiffrement IKE (Phase 1) : Diffie-Hellman : DH14 MODP Group (2048-bits) Durée de vie : 21600 Propositions : sha2_256/256,aes/256 - sha2_256/256,aes/128 Profil de chiffrement IPsec (Phase 2) : Perfect Forward Secrecy (PES) : DH14 MODP Group (2048-bits) Durée de vie : 21600				
S OBJETS	Authentification: hmac_sha256/256 Chiffrement: aes/256, aes/128 × Annuler Enregistrer				

• Cliquez sur Enregistrer* pour créer le tunnel VPN et activer la politique. ==== Profils de chiffrement ===== * Le profil de chiffrement phase 1 appelé également profil IKE est configuré au niveau du correspondant. * Le profil de chiffrement phase 2, appelé profil IPSEC est configuré au niveau du tunnel VPN.

D VPN / IPSEC VPN	
ENCRYPTION POLICY - TUNNELS	PEERS IDENTIFICATION ENCRYPTION PROFILES
🔍 Enter a filter 📃 📃	SITE FW B
 Remote gateways (1) 	General
Site_Fw_8	
	Comment
	Local address: Any
	IKE profile: StrongEncryption
	IKE version: REEVI Profil phase 1 (IKE)
	Profil phase 2 (IPSE
	Authentication method: Pre-shared key (PSK)
	F D VPN / IPSEC VPN
	F ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES
	Psec 01 (01)
	SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS
	🔍 Enter a filter 🦨 🖉 🕂 Add - 🗙 Delete 🏦 Up 🌡 Down 🖄 Cut 📑 Copy 🐑 Paste 👁 Show details
	Status = Local network Peer Remote network Encryption profile
	1 🜑 on 📲 Network_in Site_Fw_B 📲 Net_in_B StrongEncryption

Pour les deux phases, il existe trois profils préconfigurés : * StrongEncryption, * GoodEncryption * Mobile. L'onglet **PROFILS DE CHIFFREMENT** du menu **VPN** \Rightarrow **VPN IPSec** permet de : * Consulter et de modifier la configuration des profils préconfigurés, * Définir les profils qui seront utilisés par défaut lors de l'ajout des tunnels, * Créer de nouveaux profils phase 1 et phase 2 personnalisés.



A faire :

Configurez le tunnel VPN IPsec avec ces profils de chiffrement par défaut en configurant le SNS de l'autre extrémité du tunnel

===== Fonction Keepalive ===== La fonction Keepalive permet de maintenir le tunnel disponible en envoyant un paquet UDP à destination du réseau distant sur le port numéro 9, avec une certaine fréquence. Cela provoque la négociation initiale du tunnel, puis ses renégociations périodiques. Elle permet de configurer la fréquence en secondes avec laquelle les paquets UDP sont envoyés. ===== Règles du pare-feu ===== Lors de la création du tunnel VPN IPsec site-à-site, des règles implicites sont ajoutées automatiquement pour autoriser la réception du trafic constituant un tunnel VPN IPSec : les ports UDP/500, UDP/4500 et le protocole ESP. Ces règles ne concernent que les flux entrants car les flux sortants sont déjà couverts par les règles flux implicites du firewall.

SECURITY POLICY / IMPLICIT RULES			
IMPLICIT FILTER	RULES		
Enabled =	Name		
C Enabled	Allow access to the PPTP server		
C Enabled	Allow mutual access between the members of a firewall cluster (HA)		
C Enabled	Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers.		
C Enabled	Allow protected interfaces to access the firewall's DNS service (port 53).		

From: / - Les cours du BTS SIO

Permanent link: /doku.php/activiteipsec?rev=1638739917

Last update: 2021/12/05 22:31

