Fiche savoirs technologiques : Filtrage protocolaire

La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers de l'UTM Stormshield Network.

Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, ...) peuvent être activées : il s'agit du **Filtrage applicatif**.

Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise et prendre en compte les **bonnes pratiques** telles que préconisées par l'**ANSSI**.

Présentation des fonctionnalités

Pour définir un flux, une règle de filtrage se base sur de nombreux critères, ce qui offre un haut niveau de granularité.

Parmi ces critères, il est notamment possible de préciser :

- l'adresse IP source et/ou destination ;
- la réputation et la géolocalisation de l'adresse IP source et/ou destination ;
- l'interface d'entrée et/ou sortie ;
- l'adresse réseau source et/ou destination ;
- le FQDN source et/ou destination ;
- la valeur du champ DSCP ;
- le service de la couche transport TCP/UDP (n° de port de destination) ;
- le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé);
- l'utilisateur ou le groupe d'utilisateurs devant être authentifié.

Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall SNS.

Le premier paquet appartenant à chaque nouveau flux reçu par le pare-feu est confronté aux règles de filtrage **de la première à la dernière ligne**.

Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste.

Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est **bloqué** (règle n° 3 de la politique de sécurité « Block all »).

Dans les recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu publiées par l'ANSSI le 30 mars 2013, il est précisé que la règle finale qui consiste à **bloquer et journaliser** tout ce qui n'est pas autorisé par les règles précédentes doit apparaître explicitement à la fin de la politique de filtrage appliquée.

L'ajout de cette règle explicite garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de s'assurer que la trace des flux non légitimes est conservée.

✤ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(1) Block all Editer Editer Exporter												
FILTRAGE	NAT											
Rechercher			+ Nouvel	lle règle	• × s	upprimer	1.	ŧ I	📲 🖉 🔄 Cou	iper 📑 Copier	🕑 Coller \mid	≡
	État	≞ • A	ction	±•	Source		Destinatio	n	Port dest.	Protocole	Inspection de sécurité	Commentaire
🗉 Remote Ma	anagement: G	o to Syste	em - Config	guration	to setup th	e web ad	ministratio	n applic	ation access (contie	nt 2 règles, de 1 à 2)		
1	💽 on	¢) passer		* Any		📴 firewal	II_all	<pre> firewall_srv fittps </pre>		IPS	Admin from eve
2	💽 on	•	passer		* Any		💼 firewal	ll_all	* Any	icmp (requête Echo	IPS	Allow Ping fro
∃ Default policy (contient 1 règles, de 3 à 3)												
3	💽 on	•	bloquer		* Any		* Any		* Any		IPS	Block all

Les firewalls SNS utilisent la technologie **SPI (Stateful Packet Inspection)** qui leur permet de garder en mémoire l'état des connexions TCP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi **Stateful** est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de **l'initiation de la connexion**.

Les réponses faisant partie de la même connexion sont implicitement autorisées. Ainsi, nous n'avons **nul besoin d'une règle de filtrage** supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall.

La figure suivante présente l'ordre d'application des règles de filtrage et de NAT, il est important de noter que les paquets sont filtrés **avant** la phase de traduction (NAPT).

Le premier paquet reçu est confronté aux règles de filtrage des différents niveaux suivant l'ordre présenté dans la figure ci-dessus.

Dès que les éléments du paquet correspondent à une règle dans un niveau, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes.

Si aucune règle de filtrage ne correspond, le paquet est bloqué par défaut.

Dans le cas où le paquet est autorisé, il est confronté aux règles de **NAT** des différents niveaux toujours suivant l'ordre présenté ci-dessus.

- Le filtrage implicite regroupe les règles de filtrage pré-configurées ou ajoutées dynamiquement par le pare-feu pour autoriser ou bloquer certains flux après l'activation d'un service. Par exemple, une règle implicite autorise les connexions à destination des interfaces internes du pare-feu SNS sur le port HTTPS (443/TCP) afin d'assurer un accès continu à l'interface d'administration Web. Autre exemple, dès l'activation du service SSH, un ensemble de règles implicites sera ajouté pour autoriser ces connexions depuis toutes les machines des réseaux internes.
- Le filtrage global regroupe les règles de filtrage injectées au pare-feu depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- Le filtrage local représente les règles de filtrage ajoutées par l'administrateur depuis l'interface d'administration du pare-feu SNS.

Les règles implicites sont accessibles depuis le menu CONFIGURATION / POLITIQUE DE SÉCURITÉ / Règles implicites.

Chaque règle peut être activée/désactivée.

La modification de l'état de ces règles a un impact direct sur le fonctionnement des services du firewall. Pour que le service concerné fonctionne toujours, il faut s'assurer au préalable que le flux est autorisé par les règles de priorité moindre telles que globales ou locales.

Analyse des politiques prédéfinies de filtrage

La découverte des règles déjà définies dans les deux premières politiques prédéfinies de filtrage, permet de comprendre le fonctionnement des règles de filtrage sur un pare-feu Stormshield.

- Ouvrir le menu Configuration / Politique de sécurité / Filtrage et NAT / Filtrage
- Dans la liste déroulante des politiques de sécurité, choisir (1) Block all.

Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.

La règle numéro 1 autorise l'accès en https (443) et sur le port prédéfini 1300 pare-feu_srv à toutes les interfaces du pare-feu, elle permet donc l'administration à distance depuis n'importe quel réseau.

La règle numéro 2 autorise les requêtes ICMP Echo vers toutes les interfaces du pare-feu, afin de pouvoir vérifier la présence du pare-feu à l'aide des commandes ICMP.

• Dans la liste déroulante des politiques de sécurité, choisir (2) High.

Cette politique est un peu moins restrictive que la précédente, elle autorise plus de chose à partir des réseaux internes.

La règle numéro 1 autorise l'accès à des services web en http, https, dns \Rightarrow elle permet l'accès à des sites web.

La règle numéro 2 autorise l'accès à des services ftp.

La règle numéro 3 autorise l'accès à des services de messagerie en imap, smtp, pop3 elle permet l'envoi et la réception de messages.

La règle numéro 4 autorise les requêtes ICMP Echo vers n'importe quelle destination des réseaux internes, afin de pouvoir vérifier la présence du pare-feu et des services en DMZ à l'aide des commandes ICMP.

Vous remarquerez que pour toutes ces règles la colonne « Inspection de sécurité » stipule **IPS(Intrusion Prevention System)** qui est le niveau le plus élevé de filtrage avec inspection du contenu et le cas échéant blocage si l'on suspecte un comportement anormal ou une tentative d'intrusion.

Mise en place des règles de filtrage

Vous allez mettre en place une nouvelle politique de sécurité, il faudra commencer par désactiver la règle de filtrage **Pass all** et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.

Étape 1 : Copiez la politique de filtrage/NAT (1) **Block all** vers une autre politique vide où nous allons les copier les règles de NAT de la politique 5.

• Dans la liste déroulante des politiques de sécurité, choisissez (1) Block all.

FILT	RAGE	NAT								
Reche	cher			+ Nouvelle r	ègle • 🗙 Supprimer	1 1 4 2 2 20	ouper 🔄 Copier	🕑 Coller 🗒 Chercher da	ns les logs 🛛 🛱 Chercher (dans la supervision \equiv $ imes$
		État	5₹	Action =•	Source	Destination	Port dest.	Protocole	Inspection de sécurité 🖃	Commentaire
Э R	emote M	anagement:	Go to	System - Configura	tion to setup the web adm	inistration application access (cont	ient 2 règles, de 1 à 2)			
1	⊞	💽 on		passer	Any Any	firewall_all	T firewall_srv		IPS	Admin from everywhere
2		💿 on		passer	* Any	BB firewall_all	🗷 Any	icmp (requête Echo (Ping))	IPS	Allow Ping from everywhere
E D	efault pol	licy (contier	nt 1 règ	les, de 3 à 3)						
3	-	ඟ on		bloquer	* Any	Any	Any		IPS	Block all

Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.

La règle numéro 1 autorise l'accès en **https** et sur le port prédéfini **1300 firewall_srv** à toutes les interfaces du firewall, elle permet donc l'administration à distance.

La règle numéro 2 autorise les requêtes **ICMP Echo** vers toutes les interfaces du firewall, afin de pouvoir vérifier la présence du firewall à l'aide des commandes ICMP.

- Cliquez Éditer puis copier vers et choisir une politique vide (par exemple Filter 06).
- Cliquez Sauvegarder les modifications...
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée (06) Block all. Cliquez Éditer puis Renommer et renommez-là en AgenceXBlock all & NAT, puis Mettre à jour. * Cliquez sur le bouton Appliquer puis Activer la politique "AgenceXBlock all & NAT". * Dans la liste des politiques de sécurité, choisissez la politique précédente (05) AgenceX / onglet NAT puis sélectionnez les 6 règles et cliquez sur Copier. * Dans la liste des politiques de sécurité, choisissez la politique (06) AgenceX_Block all & NAT / onglet NAT puis cliquez sur Coller. Les 6 règles de NAT/PAT sont copiées.

Étape 2 : Nous allons mettre en place une première série de règles sur le Trafic sortant. Nous vous proposons d'utiliser les bandeaux séparateurs en indiquant le rôle de chaque règle pour plus de lisibilité.

a) Votre réseau interne doit pouvoir émettre un ping vers n'importe quelle destination. * Cliquez la règle numéro 2 qui passe en surbrillance et choisissez Nouvelle règle / séparateur - Regroupement de règle.

🗄 🖃 Séparateur - regroupement de règles (contient 1 règles, de 3 à 3) 🗹 🥥

* Cliquez le symbole du crayon et modifiez le nom du séparateur en ping vers n'importe quelle destination. * Cliquez Nouvelle règle / règle simple * Action : Passer ; * Source : L'adresse IP ou le réseau source, ici Networkinternals ; * Protocole dest : laisser Any. * Double-cliquez sur Protocole et remplir les champs comme ci-dessous : * Type de protocole : Protocole IP ; * Protocole IP : icmp ; * Message ICMP : choisir au milieu de la liste requête Echo (Ping, type 8, code 0)

General							
10-000-00		PORT ET PROTOCOLE					
Action		Port					
Source		TOIL					
Destination		Port destination:	+		her		A .
Port / Protoc	cole			Alouter in outprint	ici		•
Inspection			Any				
		Protocole					
		Type de protocole:	Pro	tocole IP			•
		Protocole applicatif:	Auci	une analyse applicative			
		Protocole IP:	icm	ιp			* =
		Message ICMP:	req	uête Echo (Ping)			*
a nouvelle rè	ale se prése	nte ainsi :	2	Suivi des états (statefi			
a nouvelle rè i ping vers n'in ³ ⁴ Double-cliqu éseau interne Ajoutez un sép	egle se prése importe quelle de for off Jez sur le bou e doit pouvoi parateur non	nte ainsi : stination depuis réseau interne (passer BB Netw Jton off pour passer la r accéder aux serveurs nmé Accès aux serveurs	contient 1 règles, oric internals règle à l'état privés de la urs DMZ, ch	de 3 à 3) 🗹 🥥 Tany con, puis cliquez App DMZ (DNS, WEB (por oisissez Nouvelle rè	Diquer puis Ou rts 80 et 808 pot ègle / séparate	icmp (requête Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement d)) e. b) Vot SMTP). * de règic
a nouvelle rè ji ping vers n'il 3 Double-cliqu éseau interne kjoutez un sép puis éditez-le.	egle se prése importe quelle de log off uez sur le bou e doit pouvoi parateur non .* Cliquez N	Iton off pour passer aux serveus accéder aux serveus mé Accès aux serveus puvelle règle /règle s	contient 1 règles, ork internals règle à l'état privés de la urs DMZ, ch imple * Act	de 3 à 3) 🗹 🕥 T any con, puis cliquez App DMZ (DNS, WEB (por poisissez Nouvelle rè ion : Passer ; * Sour	D Any pliquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et 9 ur - Regroupement n ; * Destination : sr	. b) Vot 5MTP). * de règic vftppriv
a nouvelle rè ping vers n'in Double-cliqu éseau interne joutez un sép puis éditez-le. Port dest : Po	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non . * Cliquez No Port destina	nte ainsi : stination depuis réseau interne (passer BB Nerw Jton off pour passer la la r accéder aux serveurs nmé Accès aux serveurs puvelle règle /règle s tion, ici ftp. mient 2 règles de 4 à 5)	contient 1 règles, ork_internels règle à l'état privés de la urs DMZ, ch imple * Act	de 3 à 3) 🗹 🕥 any con, puis cliquez App DMZ (DNS, WEB (por loisissez Nouvelle rè ion : Passer ; * Sour	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement (n ; * Destination : sr	a. b) Vot SMTP). * de règle vftppriv
a nouvelle rè ii ⊒ ping vers n'ii 3 5 Double-cliqu éseau interne Ajoutez un sép puis éditez-le. Port dest : Port ⊒ Accès aux s	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non . * Cliquez No Port destina serveurs DMZ (co	Iton off pour passer aux serveus nmé Accès aux serveus tion, ici ftp.	contient 1 règles, oric internals règle à l'état privés de la urs DMZ, ch imple * Act	Suivi des états (statef de 3 à 3) 🔮 🕥 T any con, puis cliquez Apg DMZ (DNS, WEB (por obisissez Nouvelle rè ion : Passer ; * Sour	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement o n ; * Destination : sro	e. b) Vot SMTP). * de règle /ftppriv
a nouvelle rè i ping vers n'in 3 Double-cliqu éseau interne Ajoutez un sép puis éditez-le. Port dest : Port Accès aux s 4 Cliquez sur C * Destinatio	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non . * Cliquez No cort destina serveurs DMZ (co fi Copier puis fi on : srvhttp	Inte ainsi : stination depuis réseau interne (passer BB Nerw Jton off pour passer la r accéder aux serveurs nmé Accès aux serveurs nmé Accès aux serveurs puvelle règle /règle s tion, ici ftp. Intient 2 règles, de 4 à 5) passer Pals Nerv Coller pour créer la deu priv * Port dest : Por	contient 1 règles, ork_internels règle à l'état privés de la ars DMZ, ch imple * Act vork.in uxième règle t destinatio	Sulvi des états (statef de 3 à 3) 🗹 🕥 Tany con, puis cliquez App DMZ (DNS, WEB (por ioisissez Nouvelle rè ion : Passer ; * Sour con: Passer ; * Sour e à partir de la précéc con, ici http	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Network <i>ir</i> dente : * Action	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement (n ; * Destination : sro : Passer ; * Source :	a. b) Vot SMTP). * de règle <i>(ftppriv</i> Networ
a nouvelle rè ii ⊒ ping vers n'ii 3 Double-cliqu éseau interne ijoutez un sép puis éditez-le. Port dest : Port ⊒ Accès aux s 4 Cliquez sur C * Destination 5	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non . * Cliquez No cort destina serveurs DMZ (co copier puis co on : srvhttp	Inte ainsi : stination depuis réseau interne (passer BB Network Lton off pour passer la ir accéder aux serveurs nmé Accès aux serveurs Coller pour créer la deu priv * Port dest : Por	contient 1 règles, ork_internals règle à l'état privés de la urs DMZ, ch imple * Act vork_in uxième règle t destination	Sulvi des états (statef de 3 à 3) (any con, puis cliquez App DMZ (DNS, WEB (por poisissez Nouvelle rè ion : Passer ; * Sour (a partir de la précéc con, ici http (sry_web_priv	Diquer puis Ou rts 80 et 808 pou egle / séparate rce : Networkin dente : * Action	icmp (require Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement (n ; * Destination : sru : Passer ; * Source :	a. b) Vot SMTP). * de règle <i>vftppriv</i>
a nouvelle rè ji gipig vers n'ii 3 Double-cliqu éseau interne Joutez un sép puis éditez-le. Port dest : Pa Gort dest : Pa Cliquez sur C 5 5 5 5 5 5 5 5 5 5 5 5 5	egle se prése importe quelle de le off e doit pouvoi parateur non e doit pouvoi parateur non e cort destina serveurs DMZ (co on : srvhttp copier puis (copier puis (copier puis (copier puis (copier puis (copier puis (workin ; * E	nte ainsi : stination depuis réseau interne (passer BB Network uton off pour passer la r accéder aux serveurs nmé Accès aux serveurs nmé Accès aux serveurs puvelle règle /règle s tion, ici ftp. mtient 2 règles, de 4 à 5) passer BB Network Coller pour créer la deut priv * Port dest : Port passer BB Network Coller pour créer la troi passer BB Network Coller pour créer la troi	contient 1 règles, ork_intemals règle à l'état privés de la urs DMZ, ch imple * Act vork_in uxième règle t destination ork_in isième règle priv ; * Port	Sulvi des états (statef de 3 à 3) 🖸 🕥 any con, puis cliquez App DMZ (DNS, WEB (por loisissez Nouvelle rè ion : Passer ; * Sour e à partir de la précéc on, ici http fe sry_web_priv pour le webmail à pa dest : Port destina	Diquer puis Ou rts 80 et 808 por ègle / séparate rce : Networkin dente : * Action	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et 9 ur - Regroupement (a ; * Destination : sru : Passer ; * Source : dente : * Action : Pass ail (port TCP 808).	. b) Vot SMTP). * de règie /ftppriv Networ
a nouvelle rè ping vers n'in 3 Double-cliqu éseau interne ajoutez un sép port dest : Port Accès aux s 4 Cliquez sur C 5 Cliquez sur C 5 Cliquez sur C 5 Cliquez sur C	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur nom .* Cliquez No cort destina serveurs DMZ (co on : srvhttp copier puis (on : srvhttp Copier puis (workin ; * E	nte ainsi : stination depuis réseau interne (passer BB Nerw Lton off pour passer la r accéder aux serveurs nmé Accès aux serveurs nmé Accès aux serveurs nuél règle /règle s tion, ici ftp. mient 2 règles, de 4 à 5) passer Port dest : Por Coller pour créer la deu priv * Port dest : Por passer Port dest : Por Desser Port dest : Por passer Port dest : Por	contient 1 règles, ork_internels règle à l'état privés de la ars DMZ, ch imple * Act vark_in uxième règle t destination ork_in isième règle priv ; * Port vark_in	Sulvi des états (statef de 3 à 3) 🖸 🕥 any con, puis cliquez App DMZ (DNS, WEB (por oisissez Nouvelle ré ion : Passer ; * Sour a partir de la précéc on, ici http f srv_web_priv pour le webmail à pa dest : Port destina g sry_web_priv	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin dente : * Action 2 http artir de la précéc ation, ici webmai	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et 9 ur - Regroupement (n ; * Destination : sro : Passer ; * Source : dente : * Action : Pass ail (port TCP 808).	b) Vot SMTP). * de règle oftppriv
a nouvelle rè ii ⊒ ping vers n'ii 3 5 Double-cliqu éseau internet ijoutez un sép puis éditez-le. Port dest : P ⊒ Accès aux s 4 5 Cliquez sur C 5 6 5 Cliquez sur C 6 6 7 Cliquez sur C 2 Accès aux s 4 6 6 7 Cliquez sur C 7 Cliquez sur C 7 Source : Netw	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non . * Cliquez No Port destina serveurs DMZ (co fon : srvhttp fon : srvhttp fon ff Copier puis (workin ; * E fon ff Copier puis (copier))	Inte ainsi : stination depuis réseau interne (passer BB Network Lton off pour passer la ir accéder aux serveurs nmé Accès aux serveurs nmé Accès aux serveurs nutient 2 règles, de 4 à 5) passer PB Network Coller pour créer la deu priv * Port dest : Por passer PB Network Coller pour créer la tron Destination : srvhttpp passer PB Network Coller pour créer la qua passer PB Network Coller pour créer la qua	contient 1 règles, ork_internals règle à l'état privés de la urs DMZ, ch imple * Act uxième règle t destination isième règle priv ; * Port ork_in atrième règle : srvmailpr	Sulvi des états (statef de 3 à 3) 🖉 🕥 any con, puis cliquez App DMZ (DNS, WEB (por toisissez Nouvelle rè ion : Passer ; * Sour a partir de la précéc con, ici http fe srv_web_priv pour le webmail à pa dest : Port destina fi srv_web_priv e pour le serveur mai fiv ; * Port dest : Po	Diquer puis Ou rts 80 et 808 pou àgle / séparate rce : Networkin dente : * Action <u>*</u> http artir de la précéc ation, ici webma * webmail il smtp à partir d ort destination	Icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement on ; * Destination : sru : Passer ; * Source : dente : * Action : Pass ail (port TCP 808). e la précédente : * Act , ici smtp.	b) Vot SMTP). * de règle /ftppriv Networ
La nouvelle rè i ping vers n'il 3 ⁶ Double-cliqu éseau interne Ajoutez un sép pous éditez-le. Port dest : Po ¹ Accès aux s ⁴ ⁶ Cliquez sur (⁵ ⁶ Cliquez sur (⁶ Cliquez sur (⁷ Cliquez sur (⁷ Cliquez sur (⁷ Cliquez sur (⁷ Cliquez sur (⁶ Cliquez sur (⁷ Cliquez sur (egle se prése importe quelle de co off uez sur le bou e doit pouvoi parateur non e doit pouvoi fort destina serveurs DMZ (co co off Copier puis of workin ; * E copier puis of urce : Networkin	Accès aux serveus arte ainsi : stination depuis réseau interne (passer BB Network uton off pour passer la r accéder aux serveurs nmé Accès aux serveurs ouvelle règle /règle s ation, ici ftp. mtient 2 règles, de 4 à 5) passer B Network Coller pour créer la deu priv * Port dest : Por passer B Network Coller pour créer la tro pestination : srvhttpp passer B Network Coller pour créer la qua vorkin ; * Destination	contient 1 règles, ork_intemals règle à l'état privés de la urs DMZ, ch imple * Act vark_in uxième règle t destination risième règle priv ; * Port vark_in atrième règle cork_in	Sulvi des états (statef de 3 à 3) () any con, puis cliquez App DMZ (DNS, WEB (por oisissez Nouvelle rè ion : Passer ; * Sour e à partir de la précéc on, ici http fe srv_web_priv pour le webmail à pa dest : Port destina fi srv_web_priv e pour le serveur mai riv ; * Port dest : Por	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin dente : * Action if http artir de la précéd ation, ici webmai il smtp à partir d port destination if smtp	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et 9 ur - Regroupement (i, * Destination : sru : Passer ; * Source : dente : * Action : Pass ail (port TCP 808). e la précédente : * Act , ici smtp.	b) Vot SMTP). * de règle <i>oftppriv</i> Networ er ; * Eson :
a nouvelle rè je ping vers n'in 3 Double-cliqui éseau interne Ajoutez un sép Douts éditez-le. Port dest : Pr J Accès aux s 4 Cliquez sur C 5 Cliquez sur C 5 Cliquez sur C 6 Cliquez sur C 2 asser ; * Son 7 c) Seul votre s DNS de Google ; *	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur nom .* Cliquez Ne Port destina serveurs DMZ (co in : srvhttp copier puis (copier puis (workin ; * E copier puis (burce : Netw coff copier puis (burce : Netw coff serveur DNS le (8.8.8.8).*	Inte ainsi : stination depuis réseau interne (passer BB Network Lton off pour passer la r accéder aux serveurs nmé Accès aux serveurs nmé Accès aux serveurs numé Accès aux serveurs nué Accès aux serveurs serveurs nué Accès aux serveurs s	contient 1 règles, ork_internels règle à l'état privés de la ars DMZ, ch imple * Act vork_in uxième règle t destination tork_in atrième règle <i>: srvmailpr</i> ork_in era autorisé le /règle sin asudp.	Sulvi des états (statef de 3 à 3) 🖸 🕥 any con, puis cliquez App DMZ (DNS, WEB (por toisissez Nouvelle rè ion : Passer ; * Sour apartir de la précéc on, ici http fe arv_web_priv pour le webmail à pa dest : Port destina dest : Port destina fiv ; * Port dest : Por a résoudre vers l'ext mple * Action : Pass	Diquer puis Ou rts 80 et 808 pou ègle / séparate rce : Networkin dente : * Action t http artir de la précéc ation, ici webmai t webmail di smtp à partir d port destination t smtp érieur, et plus pi ser ; * Source :	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement (n ; * Destination : sru : Passer ; * Source : dente : * Action : Pass ail (port TCP 808). e la précédente : * Act , ici smtp. récisément vers l'IP pu srvdnspriv ; * Destin	blique d ation :
La nouvelle rè ii 🖬 ping vers n'ii 3 ^c Double-cliqu réseau interne Ajoutez un sép Duis éditez-le. Port dest : Pi I Accès aux s 4 ^c Cliquez sur C 5 ^c Cliquez sur C 5 ^c Cliquez sur C 5 ^c Cliquez sur C 7 ^c Seul votre s DNS de Google DNS de Google ; * I Résolution D	egle se prése importe quelle de lez sur le bou e doit pouvoi parateur non , * Cliquez Ne Port destina serveurs DMZ (co copier puis (copier pu	ente ainsi : stination depuis réseau interne (passer BB Netw Lton off pour passer la r accéder aux serveurs nmé Accès aux serveurs passer PB Netw Coller pour créer la qua rorkin ; * Destination passer PB Netw interne (172.16.x.10) s Cliquez Nouvelle règi Port destination, ici dn sgles, de 6 à 6)	contient 1 règles, ork_internals règle à l'état privés de la urs DMZ, ch imple * Act vork_in uxième règle t destination ork_in atrième règle <i>: srvmailpr</i> ork_in era autorisé le /règle sin ssudp.	Sulvi des états (statef de 3 à 3) 🚺 🕥 Ton, puis cliquez App DMZ (DNS, WEB (por poisissez Nouvelle rè ion : Passer ; * Sour e à partir de la précéc on, ici http Tel srv_web_priv pour le webmail à pa dest : Port destina dest : Port destina fiv ; * Port dest : Por le srv_web_priv a résoudre vers l'ext mple * Action : Pass	Diquer puis Ou rts 80 et 808 pou egle / séparate rce : Networkin dente : * Action <u>* http</u> artir de la précéc ation, ici webma il smtp à partir d ort destination <u>* smp</u> rérieur, et plus p ser ; * Source :	icmp (requète Echo (Ping i, activer la politique ur le webmail), FTP et S ur - Regroupement de i, * Destination : sru : Passer ; * Source : dente : * Action : Pass tail (port TCP 808). e la précédente : * Act , ici smtp. récisément vers l'IP pu srvdnspriv ; * Destin	blique d

Double cliquez sur le symbole off des règles pour les passer à l'état on, puis cliquez Appliquer et Oui, activer la politique. Les règles actuellement mises en place sont les suivantes :

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

R (6) Agence	A_ Block all & NA	T 🔹 📔 Editer 👻 🛛	"≟ Exporter 0				
FILT	RAGE	NAT						
Rech	ercher		+ Nouvelle règ	le 🔹 🗙 Supprimer 🕇	🔹 🧩 💣 🖻 Coupe	er 💽 Copier	🐑 Coller \mid 📮 Chercher d	ans les logs 🛛 🛱 Chercher
		État ≞•	Action =*	Source	Destination	Port dest.	Protocole	Inspection de sécurité 🖃
Ξ	Remote M	anagement: Go to	System - Configuration	on to setup the web administrat	ion application access (contient	2 règles, de 1 à 2)		
1	⊞	🜑 on	passer	* Any	ne firewall_all	Image: firewall_srv Image: firewall_srv Image: firewall_srv		IPS
2	E	C on	passer	Any	Be firewall_all	* Any	icmp (requête Echo (Ping))	IPS
Э	ping vers r	l'importe quelle de	stination depuis rése	au interne (contient 1 règles, <mark>d</mark> e	:3 à 3)			
3	E	💿 on	passer	B Network_internals	* Any	* Any	icmp (requête Echo (Ping))	IPS
Ξ.	Accès aux	serveurs DMZ (co	ntient 4 règles, de 4 i	à 7)				
4		💽 on	passer	며 Network_in	I srv_ftp_priv	T ftp		IPS
5		on 🔍	passer	Pa Network_in	srv_web_priv	I http		IPS
6		on	passer	P Network_in	srv_web_priv	İ webmail		IPS
7	E	💿 on	passer		srv_mail_priv	T smtp		IPS
Ξ	Résolution	DNS (contient 1 r	ègles, de 8 à 8)					
8	⊞	💽 on	passer	srv_dns_priv	FWOUT_Siege	T dns_udp		IPS
Э	Default po	licy (contient 1 règ	les, de 9 à 9)					
9	-	💿 on	bloquer	Any Any	Any Any	Any		IPS

Étape 3 : Vous allez mettre en place une deuxième série de règles sur les trafics entrants et sortants qui respecteront le cahier des charges ci-dessous (utilisez les séparateurs en indiquant le rôle de chaque règle).

==== Trafics sortants : ==== * Votre réseau interne (DMZ incluse) doit pouvoir joindre les serveurs FTP et Web de vos voisins. * Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine est 192.168.x.200. * Votre serveur de messagerie peut envoyer des mails vers les serveurs publiés par vos voisins. * Votre réseau interne, à l'exception de vos serveurs en DMZ, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec www.visitkorea.or.kr). * L'accès au site https://www.cnn.com doit être bloqué depuis le réseau interne, en utilisant un objet FQDN. === Trafics entrants : ==== * Les utilisateurs de l'autre agence peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés. * Le serveur mails de l'autre agence est autorisés à transmettre des emails à votre serveur de messagerie * Les utilisateurs de l'autre agence sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure. * Le formateur est autorisé à pinger l'interface externe de votre SNS. * Les utilisateurs de l'autre agence peuvent se connecter à votre SNS : via l'interface web et en SSH. Ces événements devront lever des alarmes majeures. ==== Retour Accueil Stormshield ===== * Stormshield

From: / - Les cours du BTS SIO

Permanent link: /doku.php/fiche7filtrageprotocolaire?rev=1665474913

Last update: 2022/10/11 09:55

