EXTRANET - Firewall IP Flux Management

BCSS REF : V1/V1/2013.0050/FR/NL/EXTRANET.FIREWALL.FLUX.MANAGEMENT/2.00

Toelichting in NL: Het volstaat de velden aan te kruisen, alle gegevens correct in te vullen en het ingevulde formulier terug te sturen naar :

Explication en FR :.Pour ce faire, il vous suffit de cocher les champs qui vous conviennent, de remplir correctement toutes les données et de renvoyer le formulaire signé à :

Smals Supervision

Tel. : 02/ 787.59.65 ***E-mail :*** *supervision@smals-mvm.be*

Action / Actie	☐	**Ouverture / Opening**	☐	**Fermeture / Sluiten**

Institution demanderesse / Aanvragende instelling	
Institution qui donne l'accès/ Instelling die de toegang verleent[1]	

Description de l'application /du projet et motivation de l'ouverture de flux dans le cadre de cette application / ce projet/[2] **Beschrijving van de toepassing / het project en motivering voor de opening van de stroom in het kader van deze toepassing / dit project :**	

Références / Referenties	**Date de réalisation souhaitée / Gewenste uitvoeringsdatum :**	
	Gestionnaire client / Klantbeheerder :	
	Chef de projet technique / Technische projectleider	
	Référence dossier exploitation / Referentie exploitatiedossier:	
	Code d'imputation / Imputatiecode :	

[1] Il s'agit de l'institution qui donne accès à ses systèmes ou à ses données.
Smals n'est jamais le propriétaire des systèmes ou des données. /
Dit is de instelling die bijvoorbeeld toegang geeft tot haar systemen of gegevens,
Smals is nooit de eigenaar van systemen of gegevens.

[2] Description détaillée de l'application concernée par l'ouverture de portes à travers les firewalls. En cas d'ouverture de flux relatif(s) uniquement à des utilisateurs, la description peut faire référence à l'utilisation d'un protocole particulier (Http, Https, PoP3…).
Gedetailleerde beschrijving van de toepassing waarvoor de opening van een poort in de firewall gevraagd wordt. Voor de opening van stromen die uitsluitend betrekking hebben op gebruikers kan in de beschrijving worden verwezen naar het gebruik van een specifiek protocol (http, https, PoP3, …).

Description / Beschrijving / Description									
Source				*Destination*				*Protocol used*	*Description (if not enough place please use nota below)*
Name	*IP (Internal)*	*IP (NAT)*	*Port*	*Name*	*IP (Internal)*	*IP (NAT)*	*Port*		

Nota(s) :

Institution demanderesse / Aanvragende instelling			
Conseiller en sécurité ou son adjoint / Veiligheidsconsulent of zijn adjunct		**Responsable technique / Technisch verantwoordelijke**	
Date / Datum		Date/Datum	
E-mail		E-mail	
Signature / Handtekening		Signature / Handtekening	

Institution qui donne l'accès / Instelling die de toegang verleent			
Conseiller en sécurité ou son adjoint / Veiligheidsconsulent of zijn adjunct		**Responsable technique / Technisch verantwoordelijke**	
Date / Datum		Date/Datum	
E-mail		E-mail	
Signature / Handtekening		Signature / Handtekening	

POUR RAPPEL : SMALS N'EST PAS L'INSTITUTION QUI DONNE ACCES !
TER HERINNERING : SMALS IS NIET DE INSTELLING DIE TOEGANG VERLEENT !

RECOMMANDATIONS

Pour rappel : Seuls les flux HTTP/FTP et les flux SMTP sont soumis à un scanning anti-virus.

Rappelons également que le protocole utilisé par votre application lui est propre et ne peut être inspecté par les outils standards utilisés pour la sécurité du réseau. En conséquence, si le firewall autorise le passage du trafic sur une porte particulière, ouverte à votre demande, il n'inspecte pas le contenu des paquets autorisés.

Toutes les mesures doivent donc être prises au niveau des serveurs de votre institution pour garantir leur sécurité. Il vous incombe donc de vérifier la vulnérabilité de vos serveurs sur les portes ouvertes et de traiter les accès illégaux. Tous les services ouverts sur ces serveurs doivent donc être sécurisés même si certains de ces services ne sont pas accessibles depuis l'extérieur.

En outre, les firewalls de l'extranet exercent une protection périphérique, à la frontière de nos réseaux avec le monde extérieur. Ils ne peuvent rien contre une attaque développée en interne dans votre institution ou relayée à partir d'une de vos machines internes vers vos serveurs ou votre réseau.

L'application visée par ces portes doit donc être conçue de façon à éviter que ce point d'entrée ne puisse être utilisé à mauvais escient (p.ex : il faut s'assurer que l'utilisateur ne puisse faire que ce qui est strictement prévu par l'application et éviter que l'utilisateur puisse accéder à des répertoires ou des données pour lesquels il n'a pas d'autorisation.)

Soulignons également que l'augmentation du nombre de flux est préjudiciable à la sécurité. Il est donc nécessaire de s'assurer d'une part de la nécessité absolue de l'ouverture du flux et d'autre part d'étudier toutes solutions alternatives possibles (utilisation de flux et de services existants).

AANBEVELINGEN

Ter herinnering: Enkel HTTP/FTP-stromen en SMTP-stromen worden onderworpen aan antivirus-scanning.

Het protocol dat door uw toepassing gebruikt wordt is eigen aan uw toepassing en kan dus niet worden gecontroleerd door de standaardtools die voor de veiligheid van het netwerk worden gebruikt. Als de firewall bijgevolg de communicatie op een bepaalde poort toelaat, die op uw vraag werd geopend, dan wordt de inhoud van de toegelaten pakketten niet gecontroleerd.

Het is dus belangrijk om alle noodzakelijke maatregelen te treffen op het niveau van de servers van uw instelling teneinde de veiligheid ervan te garanderen. Het is uw verantwoordelijkheid om de kwetsbaarheid van uw servers op de open poorten te controleren en de ongewettigde toegangen aan te pakken. Alle diensten die op deze servers geopend worden moeten dus beveiligd zijn, ook al zijn deze diensten niet toegankelijk van buitenaf.

De firewalls van het extranet verzekeren bovendien een perifere beveiliging op de grens van onze netwerken met de buitenwereld. Ze kunnen niets tegen een aanval die van binnenuit ontwikkeld werd in uw instelling of die gelanceerd werd vanaf één van uw interne machines naar uw servers of uw netwerk.

De toepassing waarvoor deze poorten geopend worden dient zo ontworpen te zijn dat er geen misbruik kan worden gemaakt van dit toegangspunt (men moet er bv. op toezien dat de gebruiker enkel datgene kan doen waarvoor de toepassing strikt ontworpen werd en vermijden dat de gebruiker toegang krijgt tot bestanden of gegevens waarvoor hij geen toelating heeft).

Er dient ook op gewezen te worden dat de toename van het aantal stromen de veiligheid in gevaar brengt. Het is dan ook belangrijk om zich te vergewissen van de absolute noodzaak om stromen te openen en na te gaan of er geen alternatieve oplossingen mogelijk zijn (gebruik van bestaande stromen en diensten).