IT Essentials 5.0

10.3.1.8 Travaux pratiques – Configuration d'un pare-feu sous Windows 7

Imprimez et faites ces travaux pratiques.

Au cours de ces travaux pratiques, vous allez explorer le pare-feu Windows 7 et configurer quelques paramètres avancés.

Matériel conseillé

- Deux ordinateurs connectés directement ou par le biais d'un concentrateur ou d'un commutateur
- Windows 7 installé sur les deux ordinateurs
- Ordinateurs appartenant au même groupe de travail et partageant le même masque de sous-réseau

Étape 1

Sur l'ordinateur 1, cliquez avec le bouton droit sur le bureau et sélectionnez Nouveau > Dossier.



Baptisez le dossier « Cisco ».

Cliquez avec le bouton droit sur le dossier **Cisco**, puis sélectionnez **Partager avec > Partage avancé > Partage avancé**.

La fenêtre « Partage avancé » s'affiche.

Partage de fichiers et de dossie Cisco Partagé Chemin réseau : \WIN-7C01LBJHS91\Cisco Partage avancé Définir des autorisations person	tage avancé
d'autres options de partage. Protection par mot de passe Les utilisateurs doivent posséd cet ordinateur pour accéder au Pour modifier ce paramètre, util	Limiter le nombre d'utilisateurs simultanés à : 20 🗼 Commentaires : Autorisations Mise en cache OK Annuler Appliquer

Partagez le dossier et utilisez le nom par défaut Cisco.

Sur l'ordinateur 2, cliquez sur **Démarrer > Panneau de configuration > Centre Réseau et partage >** icône **Réseau**.

Double-cliquez sur l'ordinateur 1.

🕒 🗢 📭 🕨 Rése	WIN-7C01LBJHS > - 49 Rechercher dans	WIN-7CO1LBJHS	591 🔎
Organiser 👻 Centre I	éseau et partage Afficher les imprimantes distantes	₩ = ▼ □	0
 Bibliothèques Documents Images Musique Vidéos 	Cisco Partage XP Folder Partage		
『특 Ordinateur 🏜 Disque local (C:) 😴 data (\\vn-server2)	•		
2 élément(s)			

Pouvez-vous voir le dossier partagé Cisco ?

Remarque : si vous avez répondu non, demandez à l'instructeur de vous aider.

Fermez Réseau.

Remarque : sauf indication contraire, continuez le TP avec l'ordinateur 1.

Accédez au pare-feu Windows 7 :

Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Pare-feu Windows**.



Le témoin du pare-feu indique son état. Il est Activé par défaut

Dans l'espace ci-dessous, citez les avantages du pare-feu Windows.

Cliquez sur Autoriser un programme ou une fonctionnalité via le Pare-feu Windows.



Étape 4

La fenêtre « Programmes autorisés » s'affiche.

🕞 🔵 🗢 📽 « Pare-feu Windows 🕨 Programmes autorisés	 ✓ ✓ Rechercher
Autoriser les programmes à communiquer à tr Pour ajouter, modifier ou supprimer des programmes et des paramètres. Quels sont les risques si un programme est autorisé à commu	ravers le Pare-feu Windows ports autorisés, cliquez sur Modifier les uniquer ? Modifier les paramètres
New	Demesting (astronic (asis) Dublis
Nom	Domestique/entreprise (prive) Public
Assistance a distance	
BranchCache - Client de mise en cache neberge (duils.	
BranchCache - Extraction du contenu (utilise HTTP)	
BranchCache - Serveur de cache béhergé (utilise HTT	
Bureau à distance	
Connexion à un projecteur réseau	
Coordinateur de transactions distribuées	
Gestion à distance de Windows	
Gestion à distance des journaux des événements	
Gestion à distance des tâches planifiées	
Gestion à distance du Pare-feu Windows	
	Détails Supprimer
	Autoriser un autre programme
	OK Annuler

Les programmes et services que le pare-feu Windows ne bloque pas sont cochés dans la liste.

Vous pouvez ajouter des applications à cette liste. Cela peut être nécessaire si votre client dispose d'une application qui nécessite des communications avec l'extérieur, et que le pare-feu Windows, pour une raison quelconque, ne parvient pas à effectuer automatiquement la configuration. Vous devez ouvrir une session en tant qu'administrateur sur l'ordinateur pour exécuter cette procédure.

Cliquez sur Quels sont les risques si un programme est autorisé à communiquer ?.

La fenêtre « Aide et support Windows » s'affiche.

Aide et support Windows					• x
		۱	ad 🚺	<u> D</u> emander (Options 🔻
	Rechercher dans l'Aide		٩		
Quels sont les risques enc Lorsque vous ajoutez un program feu, vous autorisez un programme Autoriser un programme à comm pare-feu.	ourus lorsque vous autorise me à la liste des programmes autori : particulier à envoyer des informatie uniquer à travers un pare-feu (parfo	ez des programı sés dans un pare-feu, ons à ou depuis votre is appelé <i>déblocage</i>)	mes à franch , ou lorsque vou : ordinateur à tra revient à percer	ir un pare-feu ? s ouvrez un port de p avers ce pare-feu. un petit trou dans ur	pare-
Chaque fois que vous ouvrez un p peu plus vulnérable. Plus votre pa les pirates informatiques ou les los ou utiliser votre ordinateur pour re	ort ou autorisez un programme à co re-feu comporte de programmes au giciels malveillants d'utiliser l'une de épandre des logiciels malveillants.	ommuniquer à traver itorisés ou de ports o e ces ouvertures pour	s un pare-feu, vo uverts, plus il exi répandre un ver	otre ordinateur devie iste des possibilités p r, accéder à vos fichie	nt un oour ers ≣
Il est généralement plus sûr d'ajou un port, il reste ouvert jusqu'à ce o programmes autorisés, le « trou »	ter un programme à la liste des prog que vous le fermiez, qu'un programr est uniquement ouvert lorsqu'il est ·	grammes autorisés p me l'utilise ou non. Si nécessaire à une com	lutôt que d'ouvr vous ajoutez ur munication par	ir un port. Si vous ou n programme à la list ticulière.	ivrez te des
Pour réduire le risque pour la sécu	rité :				
Autorisez un programme ou o de la liste des programmes aut	uvrez un port uniquement lorsque c orisés ou fermez les ports lorsque vo	ela est vraiment néce ous n'en avez plus be	essaire et supprir soin.	mez les programmes	
N'autorisez jamais un program	me que vous ne reconnaissez pas à	communiquer à trav	ers le pare-feu.		+
A Plus d'options <u>d</u> e support			j ⊒ <u>A</u> ide e	en mode hors conne	xion 🔻

Créer trop d'exceptions dans votre fichier Programmes et services peut avoir de graves conséquences. Décrivez l'une d'entre elles.

Fermez la fenêtre Aide et support Windows.

Sur l'ordinateur 1 :

Cliquez dans la fenêtre « Programmes autorisés » afin de l'activer.

The real miniation of the grammes balances)		
Autoriser les programmes à communiquer à tra	vers le Pare-feu Window	S	
Pour ajouter, modifier ou supprimer des programmes et des pr	orts autorisés, cliquez sur Modifie	er les	
paramètres.			
Quels sont les risques si un programme est autorisé à commur	iquer ? 🛛 🔞 Modifier les	; paramèt	res
Programmes et fonctionnalités autorisés :			
Nom	Domestique/entreprise (privé)	Public	*
Assistance à distance			
BranchCache - Client de mise en cache hébergé (utilis			E
BranchCache - Découverte d'homologue (utilise WSD)			
BranchCache - Extraction du contenu (utilise HTTP)			
BranchCache - Serveur de cache hébergé (utilise HTT			
Bureau à distance			
Connexion à un projecteur réseau			
Coordinateur de transactions distribuées			
Gestion à distance de Windows			
Gestion à distance des journaux des événements			
Gestion à distance des tâches planifiées			
Gestion à distance du Pare-feu Windows			-
	Détails	Supprime	er
	Autoriser un autre p	rogramm	ie

Pour désactiver une exception, désactivez Partage de fichiers et d'imprimantes > OK.

Sur l'ordinateur 2 :

Ouvrez la connexion réseau à l'ordinateur 1.

Cliquez sur **Démarrer > Panneau de configuration > Centre Réseau et partage >** icône **Réseau**.



Pouvez-vous vous connecter à l'ordinateur 1?

Sur l'ordinateur 1 : Pour activer une exception, cochez la case **Partage de fichiers et d'imprimantes > OK**.

Sur l'ordinateur 2 : Actualisez l'écran **Réseau** et connectez-vous à l'ordinateur 1.

	► WIN-7C01LBJHS ► ► ► ► Rechercher dans : WIN-7C01LBJHS91 ₽
Organiser 👻 Centre I	Réseau et partage Afficher les imprimantes distantes 📲 🔻 🔟 🔞
 Bibliothèques Documents Images Musique Vidéos Ordinateur Disque local (C:) data (\\vn-server2) 	Cisco Partage XP Folder Partage
2 élément(s)	

Pouvez-vous vous connecter à l'ordinateur 1?

Fermez la session de l'ordinateur 2. Continuez le TP avec l'ordinateur 1.

Étape 6

Cliquez sur Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration > Pare-feu Windows avec fonctions avancées de sécurité > Règles de trafic entrant.

chier Action Affichage ?							
🔿 📶 🗟 🔽 🖬							
Pare-feu Windows avec fonctio	Règles de trafic entrant						Actions
E Régles de traîte entrant Régles de trafic sortant À Règles de sécurité de conne Analyse	Nom Journaux et alertes de performance (TCP entrant) Journaux et alertes de performance (TCP entrant) Lecteur Windows Media (UDP-Entrée) Partage de fichiers et d'imprimantes (Demande d'écho - ICMPv6 entrant) Partage de fichiers et d'imprimantes (Demande d'écho - ICMPv6 entrant) Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4) Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4) Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4) Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4) Partage de fichiers et d'imprimantes (LLMNR-UDP-In) Partage de fichiers et d'imprimantes (LLMNR-UDP-In) Partage de fichiers et d'imprimantes (NB-Datagramme-Entrée) Partage de fichiers et d'imprimantes (NB-Datagramme-Entrée)	Groupe Journaux et alertes Journaux et alertes Lecteur Windows Partage de fichiers Partage de fichiers Par	Profil Privé, Doma Tout Public Doma Privé	Acti Non Non Non Oui Non Oui Non Oui Non Oui Non Oui Non	Action Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser	•	Règles de trafi Image: Segles de trafi Image: Segles de trafi Image: Segles de trafic Imag
	Partage de fichiers et d'imprimantes (NB-Nom-Entrée) Partage de fichiers et d'imprimantes (NB-Nom-Entrée) Partage de fichiers et d'imprimantes (NB-Nom-Entrée) Partage de fichiers et d'imprimantes (NB-Session-Entrée) Partage de fichiers et d'imprimantes (NB-Session-Entrée)	Aide Partage de ticniers Partage de fichiers Partage de fichiers Partage de fichiers	Prive Public Privé Public	Non Oui Non Oui Non	Autoriser Autoriser Autoriser Autoriser Autoriser		Couper Copier Supprimer Propriétés

Développez la fenêtre de telle sorte que le nom complet des règles de trafic entrant soit visible. Recherchez Partage de fichiers et d'imprimantes (Demande d'écho – Trafic entrant ICMPv4).

Cliquez avec le bouton droit sur la règle et sélectionnez **Propriétés >** onglet **Avancé > Personnaliser**.

General	_	Programmes et se	rvices	Ordinateurs
Protocoles e	t ports	Étendue	Avancé	Utilisateurs
Profils Spe	écifiez les p Domaine Privé Public	profils auxquels cette	règle s'applique.	
Types d'inter Spe aux	faces écifier les ty quels cette	vpes d'interfaces e règle doit s'applique	er. Personn	aliser
Iraversee la La pay pér Ad Bi Bi Er dir (N	Personr Cette suivar ● Ic © Cet	naliser les types d'in règle s'applique aux i ts. sus les types d'interfa es types d'interfaces Réseau local Accès distant Sans fil	nterfaces connexions aux ty ces :	rpes d'interfaces
omations s	<u>En sa</u>	voir plus sur les types	d'interfaces	Annuler

L'onglet Avancé affiche le ou les profils utilisés par l'ordinateur et la fenêtre Personnaliser les types d'interfaces affiche les différentes connexions configurées pour votre ordinateur.

Cliquez sur OK.

Cliquez sur l'onglet Programmes et services.

La fenêtre « Personnaliser les paramètres des services » s'affiche.

Général	Étendue Ava Programmes et services	ancé Utilisateurs Ordinateurs	
rogrammes			
📕 🔘 Tous les p	rogrammes répondant aux co	onditions spécifiées	
Ce progra	mme :		
		Parcourir	
envices.			
ervices Spécifier les tr	vpes d'interfaces auxquels ce	ette règle	
doit s'applique	er.	Parametres	
P 1			
onnaliser les parame	tres des services		
oliquer cette règle com	ne suit :		
-			
Appliquer à tous les pr	ogrammes et services		
Appliquer aux services	s uniquement		
Appliquer à ce service			
Nom		Nom court	
Accès du nérinhé	rique d'interface utilisateur	hidsen	
Acces du penprie	nque u interrace utilisateur	StiSvo	
Acquisition d'image		00000	
Acquisition d'imag	on d'accès réseau	nanagent	
Acquisition d'imag	on d'accès réseau a IPeac	napagent Policy-Acent	
Agent de protecti Agent de stratégi	on d'accès réseau e IPsec	napagent PolicyAgent Power	
 Acquisition d'image Agent de protecti Agent de stratégi Alimentation 	on d'accès réseau e IPsec	napagent PolicyAgent Power Bas S	
Acquisition d'image Agent de protecti Agent de stratégi Alimentation Appel de procédu	on d'accès réseau e IPsec ure distante (RPC)	napagent PolicyAgent Power RpcSs	
Acquisition d'image Agent de protecti Agent de stratégi Alimentation Appel de procédu Application systèr	on d'accès réseau e IPsec ure distante (RPC) me COM+	napagent PolicyAgent Power RpcSs COMSysApp	
Acquisition d'image Agent de protection Agent de stratégion Alimentation Appel de procéduon Application systèm Assistance IP	on d'accès réseau e IPsec ure distante (RPC) me COM+	napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc	
Acquisition d'image Agent de protecti Agent de stratégi Alimentation Appel de procédu Application systèr Assistance IP Assistance NetBI	on d'accès réseau e IPsec ure distante (RPC) me COM+ OS sur TCP/IP	napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc Imhosts	-
Acquisition d'image Agent de protecti Agent de stratégi Agent de stratégi Appel de procédu Application systèr Assistance IP Assistance NetBl Appliquer au service p	on d'accès réseau e IPsec ure distante (RPC) me COM+ <u>OS sur TCP/IP</u> portant ce <u>n</u> om court (par exe	napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc Imhosts mple : eventlog) :	Ţ
Acquisition d'imag Agent de protecti Agent de stratégi Alimentation Appel de procédu Application systèr Assistance IP Assistance NetBl Appliquer au service p	on d'accès réseau e IPsec ure distante (RPC) me COM+ <u>OS sur TCP/IP</u> vortant ce <u>n</u> om court (par exe	napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc Imhosts	•
Acquisition d'imag Agent de protecti Agent de stratégi Alimentation Appel de procédu Application systèr Assistance IP Assistance NetBl Appliquer au service p	on d'accès réseau e IPsec ure distante (RPC) me COM+ <u>OS sur TCP/IP</u> ortant ce <u>n</u> om court (par exe	napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc Imhosts	•

Citez le nom abrégé de quatre services disponibles.

Cliquez sur Annuler.

Il existe de nombreuses applications, généralement invisibles pour l'utilisateur, qui doivent également transiter par le pare-feu pour accéder à votre ordinateur. Il s'agit de commandes au niveau du réseau chargées d'acheminer le trafic sur le réseau et sur Internet.

Cliquez sur l'onglet **Protocoles et ports**. Pour accéder aux paramètres ICMP, cliquez sur le bouton **Personnaliser**. La liste où sont configurées les exceptions ICMP s'affiche sur cette page.

Personnaliser les paramètres ICMP	×
Appliquer cette règle aux connexions ICMP (Internet Control Message Protocol) suivantes :	
Tous les types ICMP	
 Paquet trop important Destination inaccessible Extinction de source Redirection Requête d'écho Annonce de routeur Sollicitation de routeur Délai dépassé Problème de paramètre Demande d'horodatage Demande de masque d'adresses 	
Ce type ICMP : <u>Type</u> : 0	

Dans cet exemple, le fait d'autoriser les requêtes d'écho entrantes est ce qui permet aux utilisateurs du réseau d'envoyer une commande ping vers votre ordinateur afin de déterminer s'il est présent sur le réseau. Cela permet également de déterminer la vitesse de déplacement des informations vers et depuis votre ordinateur.

Dans l'espace ci-dessous, répertoriez les types ICMP spécifiques.

Fermez toutes les fenêtres.