# Travaux pratiques - Configuration du pare-feu sous Windows 8

## Introduction

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

## Matériel conseillé

- Deux ordinateurs connectés directement ou connectés via un réseau
- Windows 8 installé sur les deux ordinateurs
- Les ordinateurs doivent appartenir au même groupe de travail et partager le même masque de sousréseau

#### Étape 1 : Créez et partagez un dossier sur PC-1.

- a. Ouvrez une session sur **PC-1** en tant que membre du groupe des administrateurs. Demandez le nom d'utilisateur et le mot de passe à votre instructeur.
- b. Sur **PC-1**, cliquez avec le bouton droit sur le Bureau, puis sélectionnez **Nouveau > Dossier**. Baptisez ce dossier **Cisco**.



c. Cliquez avec le bouton droit sur le dossier Cisco, puis sélectionnez Propriétés > Partage > Partage avancé. La fenêtre Partage avancé s'affiche. Cliquez sur Partager ce dossier et utilisez le nom par défaut Cisco. Cliquez sur OK. Fermez la fenêtre Propriétés Cisco.

👢 Pre	opriétés de : Cisco
Général Partage Sécurité Pers Partage de fichiers et de dossiers Cisco Non partagé	en réseau
Chemin réseau : Non partagé Partager	Partage avancé ×
Partage avancé Définir des autorisations personn d'autres options de partage.	Paramètres Nom du partage : Cisco Ajouter Supprimer Limiter le nombre d'utilisateurs simultanés à : 20 🜩
Protection par mot de passe Les utilisateurs doivent posséder cet ordinateur pour accéder aux Pour modifier ce paramètre, utilis	Commentaires :          Autorisations       Mise en cache         OK       Annuler       Appliquer

#### Étape 2 : Utilisez l'Explorateur de fichiers pour afficher le dossier partagé sur PC-1.

- a. Ouvrez une session sur **PC-2** en tant que membre du groupe des administrateurs. Demandez le nom d'utilisateur et le mot de passe à votre instructeur.
- b. Ouvrez la fenêtre de l'**Explorateur de fichiers**. Dans le volet de gauche, sous **Réseau**, développez **PC-1**.

🥮 l 🔝 🚯 = 1	PC-1 -	×
Fichier Accueil Partage Affichage		~ <b>?</b>
🔄 🦻 ▾ ↑ 🖳 ⊦ Réseau ⊦ FR	✓ 🖒 Rechercher dans : PC-1	Q
<ul> <li>▷ INALSD-RS</li> <li>▷ INALSD-SP</li> <li>▲ INALSD-SP</li> <li>▲ INALSD-SP</li> <li>▲ INALSD-SP</li> </ul>	Cisco Partage	
▷ 🖳 PC-2 ▷ 🖳 STUDENT01		
Þ 🖳 tsclient Na≣i vista a i 1 élément	~	:== 🕥

Sous PC-1, voyez-vous le dossier partagé Cisco ?

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

c. Fermez l'Explorateur de fichiers.

#### Étape 3 : Ouvrez le pare-feu Windows sur PC-1.

Remarque : sauf indication contraire, utilisez PC-1 pour le reste de ces travaux pratiques.

a. Pour ouvrir la fenêtre Pare-feu Windows, cliquez sur Panneau de configuration > Pare-feu Windows.

b. L'état normal du pare-feu Windows est Activé.



c. Quels sont les avantages du pare-feu Windows ?


Étape 4 : Étudiez la fonctionnalité Programmes autorisés du pare-feu Windows.

a. Cliquez sur Autoriser une application ou une fonctionnalité via le Pare-feu Windows.

<b>@</b>	Pare-feu Windows	- • ×
( → → ↑ and w ≤ Système et set s	sécurité 🔸 Pare-feu Windows	✓ C Rechercher
<ul> <li>Page d'accueil du panneau de configuration</li> <li><u>Autoriser une application ou une fonctionnalité via le Pare fau Windows</u></li> <li>Modiña les paramètres de notification</li> <li>Activer ou désactiver le Pare-feu Windows</li> <li>Paramètres par défaut</li> <li>Paramètres par défaut</li> <li>Dépanner mon réseau</li> </ul>	Protégez votre ordinateur avec le Pa Le Pare-feu Windows a pour but d'empécher la votre ordinateur via Internet ou via un réseau. Réseaux à domicile ou sur un lieu de travail, o périphériques présents sur le réseau État du Pare-feu Windows : Connexions entrantes : Réseaux privés actifs : État de notification : Réseaux publics ou invités	are-feu Windows les pirates ou les logiciels malveillants d'accéder à Connecté ⊙ où vous faites confiance aux personnes et aux Activé Bloquer toutes les connexions aux applications autorisées
Voir aussi Centre de maintenance Centre Réseau et partage		

b. La fenêtre **Applications autorisées** s'affiche. Les programmes et services que le pare-feu Windows ne bloque pas sont cochés dans la liste suivante. Cliquez sur **Quels sont les risques si une application** est autorisée à communiquer ?

**Remarque** : vous pouvez ajouter des applications à cette liste. Cela peut être nécessaire si vous disposez d'une application qui nécessite des communications avec l'extérieur, et que le pare-feu Windows, pour une raison guelcongue, ne parvient pas à effectuer automatiguement la configuration.

Autoriser les applications à communiquer à travers le P Pour ajouter, modifier ou supprimer des applications et des ports autoris paramètres.	are-feu Windows és, cliquez sur Modifier	r les	
Quels sont les risques si une application est autorisée à communiquer ?	😌 Modifier les	s paramètr	es
Applications et fonctionnalités autorisées :			
Nom	Privé	Public	^
✓ Actualités		<b>V</b>	
✓ Affichage sans fil	$\checkmark$	<b>~</b>	
Analyse de l'ordinateur virtuel			
Arrêt à distance			
Assistance à distance	$\checkmark$		
☑ Bing Cuisine & vins	$\checkmark$	$\checkmark$	
☑ Bing Santé & forme	$\checkmark$	<b>v</b>	
BranchCache - Client de mise en cache hébergé (utilise HTTPS)			
BranchCache - Découverte d'homologue (utilise WSD)			
BranchCache - Extraction du contenu (utilise HTTP)			
BranchCache - Serveur de cache hébergé (utilise HTTPS)			
Bureau à distance			~
	Détails	Supprime	r

La création de trop nombreuses exceptions dans votre fichier Programmes et services peut avoir de graves conséquences.

Décrivez l'une d'entre elles.

c. Fermez la fenêtre Aide et support Windows.

Étape 5 : Configurez la fonction Applications autorisées par le pare-feu Windows.

a. Cliquez dans la fenêtre **Applications autorisées** afin de l'activer. Cliquez sur **Modifier les paramètres**. Désactivez la case à cocher **Partage de fichiers et d'imprimantes**. Cliquez sur **OK**.

$( \Rightarrow )$	<ul> <li></li></ul>	~ C	Reche	rcher		)
	Autoriser les applications à communiquer à travers le Par	e-feu Wir	ndows			
	Pour ajouter, modifier ou supprimer des applications et des ports autorisés, paramètres.	, cliquez sur	Modifier	les		
	Quels sont les risques si une application est autorisée à communiquer ?	😗 Mo	difier les	paramèt	tres	
	Applications et fonctionnalités autorisées :					
	Nom		Privé	Public	^	
	□ Journaux et alertes de performance					
	✓ JuniperNetworks.JunosPulseVpn			~		
	Lecteur Windows Media					
	✓ Liste de lectures Windows			✓		
	✓ Météo			✓		
	Moniteur d'événements distants					
	✓ Musique			✓		
	Partage de fichiers et d'imprimantes					
	Partage de proximité		لا 🗹	3 🗹		
	Périphériques mobiles sans fil					
	Protocole SSTP					
	✓ Recherche du réseau		V	✓	~	
		Détails.		Supprime	er	
		Autoriser un	e autre a	pplicatio	n	

- c. Fermez toutes les fenêtres ouvertes sur PC-2.
- d. Sur PC-1, ajoutez une coche à Partage de fichiers et d'imprimantes. Cliquez sur OK.
   Remarque : vous devriez pouvoir ajouter la coche sans avoir à cliquer sur Modifier les paramètres.
- e. Sur PC-2, rouvrez l'Explorateur de fichiers et tentez de vous connecter à PC-1.
   Pouvez-vous vous connecter à l'ordinateur 1 ? Pourquoi ?
- f. Fermez toutes les fenêtres ouvertes sur PC-2 et fermez la session.
- g. Fermez toutes les fenêtres sur PC-1.

#### Étape 6 : Configurez les fonctions de sécurité avancées du Pare-feu Windows.

**Remarque** : utilisez **PC-1** jusqu'à la fin de ces travaux pratiques.

a. Cliquez sur Panneau de configuration > Outils d'administration > Pare-feu Windows avec fonctions avancées de sécurité.

b. La fenêtre Pare-feu Windows avec fonctions avancées de sécurité s'ouvre. Dans le panneau de gauche, vous pouvez sélectionner les éléments pour configurer les Règles de trafic entrant, les Règles de trafic sortant ou les Règles de sécurité de connexion. Vous pouvez également cliquer sur Analyse pour afficher l'état des règles configurées. Cliquez sur Règles de trafic entrant.

2	Pare-feu Windows avec fonctions avancées de sécurité – 🗖 🗙
Fichier Action Affichage ?	
Pare-feu Windows avec fonctio	Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur Io Actions
<ul> <li>Règles de trafic entrant</li> <li>Règles de trafic sortant</li> <li>Règles de sécurité de conne</li> <li>Analyse</li> </ul>	Pare-feu Windows avec sécurité avancée offre une sécurité réseau poi
	Vue d'ensemble Restaurer la stratégie par défaut
	Profil de domaine Diagnostiquer / Réparer
	🔮 Le Pare-feu Windows est activé. Affichage
	S Les connexions entrantes qui ne correspondent pas à une règle sont bloqué
	V Les connexions sortantes qui ne correspondent pas à une règle sont autoris
	Le profil privé est actif
	V Le Parefeu Windows est activé.
	Les connexions entrantes qui ne correspondent pas à une règle sont bloque     Les connexions sortantes qui ne correspondent pas à une règle sont autoris
	Profil public
	V Le Pare feu Windows est activé.
	V Les connexions entrantes qui ne correspondent pas à une règle sont bloqué
	V Les connexions sortantes qui ne correspondent pas à une règle sont autoris
	Propriétés du Pare-feu Windows
	Démarrer
	Authentifier les communications entre les ordinateurs
	Créez des règles de sécurité de connexion afin de spécifier comment et quand les authentifiées et protégées à l'aide de la sécurité du protocole Internet (IPsec).
< >	Rànlas da són utá da ronnarion     V

c. Dans le volet central, faites défiler l'écran jusqu'à ce que vous trouviez la règle entrante Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4). Cliquez avec le bouton droit sur la règle, sélectionnez Propriétés, puis l'onglet Avancé.

<b>@</b>	Pare-feu Windows avec fonctions avar	ncées de s	écurité – 🗆 🗙
Fichier Action Affichage ?			
🗢 🄿 🙍 📰 🗟 🖬			
Pare-feu Windows avec fonctio	Règles de trafic entrant		Actions
Pare-feu Windows avec fonction Regles de trafic entrant Regles de trafic sortant Regles de sécurité de conne Analyse	Règles de trafic entrant         Nom       Groupe         Journaux et alertes de perform       Journaux et alertes de perform         Journaux et alertes de perform       Journaux et alertes de perform         Journaux et alertes de perform       Journaux et alertes de perform         Journaux et alertes de perform       Journaux et alertes de perform         Journaux et alertes de perform       Journaux et alertes de perform         Journaux et alertes de perform       Journaux et alertes de perform         Quartes et alertes de perform       Journaux et alertes de perform         Quartes et alertes de perform       Journaux et alertes de perform         Quartes et alertes de perform       Lecteur Windows Media & GOP         Lecteur Windows Media & GOP	Profil ^ Privé, Privé, Doma Tout Tout Doma Tout Doma Privé Doma Privé Doma Privé Doma Privé	Actions         Règles de trafic entrant       ▲         Iverse par profil       >         Filtrer par profil       >         Filtrer par groupe       >         Affichage       >         Affichage       >         Exporte la liste       >         À Affichage       >         Artice Columnation       >         Artice Columnation       >         Artice Columnation       >         Value       >         Partage de fichiers et d'imprimantes (Demande       >         Obsactiver la règle       Couper         Copier       >         Supprimer       >         Projetés       ?         Aide       >
	Partage de fichiers et d'imprim Partage de fichiers et d'impr	Public	
	Partage de fichiers et d'imprim Partage de fichiers et d'impr	Privé	
	🗑 Partage de fichiers et d'imprim Partage de fichiers et d'impr	Public 🗸	
< >	<	>	
Ouvre la boîte de dialogue des prop	riétés pour la sélection en cours.		

d. L'onglet **Avancé** affiche le ou les profils utilisés par l'ordinateur. Cliquez sur **Personnaliser** dans la zone **Types d'interfaces** de la fenêtre.

ropriétés	de : Partage	e de fich	niers et d'ir	mprima	antes (D	ema
Général	Programmes et	services	Ordinateurs	distants	Protoco	les et ports
Étendue	Avancé	Entités	de sécurité loc	ales	Utilisateu	rs distants
Profils						
	Spécifiez les pro	ofils auxqu	els cette règle	s'applique	э.	
	Domaine					
	Privé					
	Public					
Types d	'interfaces					
	Spécifier les typ cette règle doit :	es d'interfa s'appliquer	aces auxquels r.	Persor	nnaliser,	]
	ée latérale La traversée late paquets entrant périphérique de Address Transla	érale perm s non sollio périmètre, tion) ou ur	et à l'ordinateu cités qui sont p tel qu'un route n pare-feu.	ur d'accep passés par eur NAT (1	oter des • un Network	
	Bloquer la trave	ersée latér	ale		~	
	Empêcher les a directement d'le (Network Addre	pplication: nternet via ess Transla	s de recevoir d un périphériqu ation).	lu trafic no ue de périr	on sollicité mètre NAT	
			ОК	Annu	ler	Appliquer

e. La fenêtre **Personnaliser les types d'interfaces** s'affiche. Elle affiche les différentes connexions configurées sur votre ordinateur. Laissez **Tous les types d'interface** sélectionné, puis cliquez sur **OK**.

Personnaliser les types d'interfaces	×
Cette règle s'applique aux connexions aux types d'interfaces suivants.	
<ul> <li>Tous les types d'interfaces</li> </ul>	
○ Ces types d'interfaces :	
Réseau local     Accès distant     Sans fil	
OK Annuler	

f. Cliquez sur l'onglet Programmes et services. Dans la section Services, cliquez sur Paramètres.



g. La fenêtre Personnaliser les paramètres des services s'affiche.

Personnaliser les para	mètres des services		×
Appliquer cette règle comme suit :			
Appliquer à tous les programmes et services			
O Appliquer aux services uniquement			
O Appliquer à ce service :			
Nom	Nom court	^	
<ul> <li>Acquisition d'image Windows (WIA)</li> <li>Agent de protection d'accès réseau</li> <li>Agent de stratégie IPsec</li> <li>Alimentation</li> <li>Appel de procédure distante (RPC)</li> <li>Application système COM+</li> <li>Assistance IP</li> <li>Assistance NetBIOS sur TCP/IP</li> </ul>	stisvc napagent PolicyAgent Power RpcSs COMSysApp iphlpsvc Imhosts		
Appliquer au service portant ce nom court (par exemp	le : eventlog) : OK	Annuler	

- h. Citez le nom abrégé de quatre services disponibles.
- i. Cliquez sur Annuler pour fermer la fenêtre Personnaliser les paramètres des services.
- j. Cliquez sur l'onglet **Protocoles et ports**.

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

Étendue	Avancé	Entités	de sécurité locales	Utilisateurs distants
Général	Programmes et	services	Ordinateurs distants	Protocoles et ports
Protoco	les et ports			
Renade	Type de protoco	ole :	ICMPv4	~
	Numéro de prot	ocole :	1 🛓	
	Port local :		Tous les ports	~
	<b>_</b> .			
	Port distant :		Tous les ports	
	Port distant :		Tous les ports	~
	Port distant : Paramètres ICM Message Protoc	1P (Interne col) :	Tous les ports	Perso
	Port distant : Paramètres ICM Message Protoc	1P (Interne col) :	Tous les ports et Control	Perso
	Port distant : Paramètres ICM Message Protoc	IP (Interne col) :	Tous les ports	Perso
	Port distant : Paramètres ICM Message Protoc	IP (Interne col) :	Tous les ports	Perso
	Port distant : Paramètres ICM Message Protoc	IP (Interne col) :	Tous les ports	Perso
	Port distant : Paramètres ICM Message Protoc	IP (Interne col) :	Tous les ports	Perso

- k. Pour accéder aux paramètres ICMP, cliquez sur le bouton Personnaliser.
- La fenêtre Personnaliser les paramètres ICMP s'affiche. 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.

Personnaliser les paramètres ICMP	×
Appliquer cette règle aux connexions ICMP (Internet Control Message Protocol) suivantes :	
Tous les types ICMP	
Certains types ICMP	
<ul> <li>Paquet trop important</li> <li>Destination inaccessible</li> <li>Extinction de source</li> <li>Redirection</li> <li>✓ Requête d'écho</li> <li>Annonce de routeur</li> <li>Sollicitation de routeur</li> <li>Délai dépassé</li> <li>Problème de paramètre</li> <li>Demande d'horodatage</li> <li>Demande de masque d'adresses</li> </ul>	
Ce type ICMP :	
Type: 0 V Code: Tout V Ajouter	
OK Annuler	2

Dressez la liste des quatre types ICMP spécifiques.

- m. Fermez toutes les fenêtres ouvertes sur PC-1.
- n. Cliquez avec le bouton droit sur le dossier Cisco sur le Bureau, puis sélectionnez Supprimer.

# **Remarques générales**

Quelles sont les raisons possibles pour que vous deviez apporter des modifications au pare-feu ?