Hands-on Lab: Create a Firewall Rule in Microsoft Windows Defender

Estimated time needed: 30 minutes

About This Lab

This exercise will look at Windows Defender Firewall with Advanced Security. This advanced view provides more in-depth options for configuration. All Windows Firewall rules, and their details, are stored here, allowing you to edit configurations for each rule or exception.

Objectives

In this hands-on lab, you will:

- Use Windows Defender Firewall with Advanced Security to edit an existing firewall rule.
- Enforce the following rules:
- Allow the connection for Key Management Service on the Domain and Private network.
- Deny the connection for Key Management Service on the Public network.

Important Information About Lab Instructions and Solutions

In case you try to use your physical keyboard in the lab environment, it might not produce any visible results. To avoid this issue, please use the On-Screen Keyboard (you can find it by searching for On-Screen Keyboard in the search bar at the bottom of your screen). If search functionality doesn't work, you can also click on the Windows icon, scroll down to find Windows Ease of Access, click on it, and then select On-Screen Keyboard.

Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

Exercise 1: Allow an app through a firewall

1. Select the Windows Start button.





3. Select Firewall & network protection.

about:blank



4. Select Allow an app through firewall.

Windows Security

 \leftarrow _(မှ) Firewall & network \equiv 俞 Home Who and what can access your networks. O Virus & threat protection (p) Firewall & network protection App & browser control \Box 旦 Device security Public network (active)

Domain network Firewall is on. Private network Firewall is on.

protection

about:blank

Firewall is on.

Network and Internet troubleshooter

Firewall notification settings

Allow an app through firewall

Advanced settings

Restore firewalls to default

Ö Settings

5. Here you will see a list of allowed apps and features. Scroll down to Firefox (C:\Program Files\Mozilla Firefox). Notice that communication is permitted on the private, but not the public. Select the box to enable communication on the public network.

about:blank

đ

Windows Community videos

Learn more about Firewall & network protection

Who's protecting me? Manage providers

Change your privacy settings

View and change privacy settings for your Windows 10 device. Privacy settings

Privacy dashboard **Privacy Statement**

apps			_	-
			_	L
Ύ		v ⊙	Search Control Pan	el
	Allow apps to communicate through Windows Defend	der Firewall		
	To add, change, or remove allowed apps and ports, click Change settin	ngs.		
	What are the risks of allowing an app to communicate?		Change settings	
	3		÷ 2 2	1
	Allowed apps and features:			
	Name	1	Private Public ^	
	✓ Firefox (C:\Program Files\Mozilla Firefox)			
	☑ Google Chrome		V	
	iSCSI Service			
	Key Management Service			
	M mDNS			
	✓ Narrator QuickStart			
	L Netlogon Service			
	Network Discovery			
	OpenSSH Server (sshd) D			
	Performance Logs and Alerts			
	Kemote Desktop			
	Remote Desktop (WebSocket)			
		Details	Remove	
				1
		4	Allow another app	
				1
		0	K Cancel	
o acc	ent changes and to return to the Firewall and network protection	n screen		
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	_	C
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V Ö	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V C	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. v o der Firewall ngs.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. v ö der Firewall ngs.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V O der Firewall 1955.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V O der Firewall Igs.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V D der Firewall ngs.	Search Control Pan	[
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V D der Firewall ngs.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V D der Firewall Igs.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. v D der Firewall Igs.	Search Control Pan	
o acc apps	ept changes and to return to the Firewall and network protectio	n screen. V D der Firewall Igs.	Search Control Pan	el
o acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen. V D der Firewall Igs.	Search Control Pan	el
o acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen. V O der Firewall Igs.	Search Control Pan	
o acc apps 个	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	el
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	[
o acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	
o acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	[
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	[
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	[
) acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	[
) acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	
o acc apps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	
o acc apps	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	
acc ppps ↑	ept changes and to return to the Firewall and network protectio	n screen.	Search Control Pan	

Exercise 2: Enable Inbound Rules to Allow Remote Service Management

1. Select Advanced settings on the Firewall & network protection screen.

Windows Security

- ← ≡
- 命 Home
- Virus & threat protection
- ((j)) Firewall & network protection
- App & browser control
- □ Device security

(اپ) Firewall & network protection

about:blank

Who and what can access your networks.

Bo Domain network

Firewall is on.

Se Private network

Firewall is on.

Public network (active)
Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings

Restore firewalls to default

Settings
 Settings

2. Here you will see an **Overview** in the center panel. On the left side, you will see three different rule types:

- Inbound rules
 Outbound rules
- Connection security rules

These rules can be configured to filter traffic based on computers, users, applications, ports, protocols, etc. Select Inbound rules.

Windows Community videos

Learn more about Firewall & network protection

Who's protecting me? Manage providers

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings Privacy dashboard Privacy Statement

💣 Windows Defender Firewall wit	h Advanced Security		– 🗆 X
File Action View Help			
🗢 🏟 📰 🚺 🖬			
Windows Defender Firewall with	Windows Defender Firewall with Advanced Security on Local Computer		Actions
Windows Defender Firewall with	Windows Defender Firewall with Advanced Security on Local Computer Windows Defender Firewall with Advanced Security provides network security for Windows computers. Overview • Domain Profile • Windows Defender Firewall is on. • Inbound connections that do not match a rule are blocked. • Outbound connections that do not match a rule are allowed. • Private Profile • Windows Defender Firewall is on. • Inbound connections that do not match a rule are blocked. • Utbound connections that do not match a rule are allowed. • Public Profile is Active • Windows Defender Firewall is on. • Inbound connections that do not match a rule are blocked. • Windows Defender Firewall is on. • Inbound connections that do not match a rule are blocked. • Windows Defender Firewall Properties • Setting Started • Authenticate communications between computers • Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec). Connection Security Rules • <td>*</td> <td>Actions Windows Defender Firewall Import Policy Export Policy Restore Default Policy Diagnose / Repair View Refresh Properties Itelp</td>	*	Actions Windows Defender Firewall Import Policy Export Policy Restore Default Policy Diagnose / Repair View Refresh Properties Itelp
< >	View and create firewall rules Create firewall rules to allow or block connections to encotified programs or note. You can also allow a connection only # <	~	

3. Select New Rule in the right pane.

💣 Windows Defender Firewall with Advanced Security

about:blank

	_	
		_

_

File Action View Help							
🗢 🄿 🙍 📰 🗟 🛐							
Pindows Defender Firewall witl	Inbound Rules					A	ctions
Inbound Rules	Name	Group	Profile	Enabled	Action '	\ Ir	nbound Rules
Connection Security Rules	Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow		💈 New Rule
> 🛃 Monitoring	OpenSSH Server (sshd)		All	Yes	Allow	7	Filter by Profile
	✓ TightVNC		All	Yes	Allow		Filter by State
	Alloyn Router (TCP-In)	AllJoyn Router	Domai	Yes Vec	Allow	1	r Filter by Group
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Allow	1.	View
	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	Allow		Refresh
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow		Export List
	Cast to Device functionality (qWave-TCP	Cast to Device functionality	Private	Yes	Allow		Help
	Cast to Device functionality (qWave-UDP	Cast to Device functionality	Private	Yes	Allow		
	Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow		
	Cast to Device streaming server (HTTP-St	Cast to Device functionality	Private	Yes	Allow		
	Cast to Device streaming server (HTTP-St	Cast to Device functionality	Domain	Yes	Allow		
	Cast to Device streaming server (HTTP-St	Cast to Device functionality	Public	Yes	Allow		
	Cast to Device streaming server (RTCP-St	Cast to Device functionality	Private	Yes	Allow		
	Cast to Device streaming server (RTCP-St	Cast to Device functionality	Public	Yes	Allow		
	Cast to Device streaming server (RTCP-St	Cast to Device functionality	Domain	Yes	Allow		
	Cast to Device streaming server (RTSP-Str	Cast to Device functionality	Domain	Yes	Allow		
	Cast to Device streaming server (RTSP-Str	Cast to Device functionality	Private	Yes	Allow		
	Scast to Device streaming server (RTSP-Str	Cast to Device functionality	Public	Yes	Allow		
	Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow		
	COM+ Network Access (DCOM-In)	COM+ Network Access	AII	No	Allow		
	COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati	All	No	Allow		
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	Allow		
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	Allow		
	Ore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow		
	Ore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow		
< >	Core Networking - Internet Group Mana	Core Networking	All	Yes	Allow >		

4. Here you will see options for four new rule types. Select Predefined.

	v 1	
🔗 New Inbound Rule Wi	îzard	\times
Rule Type		
Select the type of firewall rule	a to create.	
Steps:		
Rule Type	What type of rule would you like to create?	
Program		
Action	Program	
Profile	Rule that controls connections for a program.	
Name	⊖ Port	
	Rule that controls connections for a TCP or UDP port.	
	O Predefined:	
	AllJoyn Router 🗸	
	Rule that controls connections for a Windows experience.	
	○ Custom	
	Custom rule.	
	< Back Next > Cancel	



about:blank

 \times

7. Check the boxes for Remote Service Management (RPC-EPMAP), Remote Service Management (NP-IN), and Remote Service Management (RPC).

💣 New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

tents for the sele exists and is che lule Exists lready exists lready exists lready exists	Next >	f group. ents of Inbou Inbou Inbou
ents for the sele exists and is che hule Exists lready exists lready exists lready exists and exists	Next >	i group. ents of Desc Inbou Inbou Noou
exists and is che lule Exists Iready exists Iready exists Iready exists	Profile All All All Next >	Desc Inbou Inbou Inbou
lule Exists Iready exists Iready exists Iready exists	Profile All All All	Desc Inbot Inbot Inbot
le Exists Iready exists Iready exists Iready exists	Profile All All All	Desc Inbou Inbou Inbou
Iready exists Iready exists Iready exists	All All All Next >	Inbor Inbor Inbor
ready exists Iready exists	All All Next >	Inbor Inbor
: Back	Next >	Cancel
K Back	Next >	Cancel
Back	Next >	Cancel
nents for the sele exists and is che	ected predefined ecked, the conte	l group. ents of
lule Exists	Profile	Desc
lready exists	All	Inbou
lready exists	All	Inbou
lready exists	All	Inbou
		>
	ule Exists Iready exists Iready exists	ule Exists Profile Iready exists All Iready exists All Iready exists All

4/29/

/25, 5:30 PM	about:blank	
9. Select Allow the connection	n if it is secure.	
💣 New Inbound Rule Wizard		Х
Action		
Specify the action to be taken whe	en a connection matches the conditions specified in the rule.	
Steps:		
 Rule Type 	What action should be taken when a connection matches the specified conditions?	
Predefined Rules		
Action	Allow the connection This includes connections that are protected with IPsec as well as those are not	
	Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Bule node	
	Customize	
	O Block the connection	
	c Back Finish Cancel	
10. Select Next.		
💣 New Inbound Rule Wizard		×
Action		
Specify the action to be taken whe	an a connection matches the conditions specified in the rule.	
Stans:		
Bule Type	What action should be taken when a connection matches the specified conditions?	
 Predefined Rules 		
Action		
Users	This includes connections that are protected with IPsec as well as those are not.	
Computers	Allow the connection if it is secure This includes ask exceedings that have been authenticated hyuning IPress. Connections	
	will be secured using the settings in IPsec properties and rules in the Connection Security	
	Customia	
	Customize	
	○ Block the connection	
	< Back Next > Cancel]

about:blank

×

11. Verify that the box to only allow connections from these users has been checked. Select Add to add an authorized user.

💣 New Inbound Rule Wizard	
Users	

Specify the users that are allowed to make the connection specified by this rule.

Steps:	Authorized upper
Rule Type	Inly allow connections from these users
Predefined Rules	Add
Action	
Users	Remove
Computers	
	Exceptions
	Add
	Nemove
	Note: user identities can only be verified if an authentication method that carries user identity is used.
	< Back Next > Cancel

12. Enter "Administrator" into the Enter the object names to select box.

Select Users or Groups		×
Select this object type:		
From this location:		Object Types
EC2AMAZ-J5GP1U8		Locations
Enter the object names to select (<u>examples</u>):		
		Check Names
Advanced	OK	Cancel

13. Select OK.

Select Users or Groups	×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
EC2AMAZ-J5GP1U8	Locations
Enter the object names to select (examples):	:
Administrator	Check Names
I	
Advanced	OK Cancel

×

14. Click Next and Select Finish. Prev Inbound Rule Wizard

Computers

Specify the computers that are allowed to make the connection specified by this rule.

Steps: Predefined Rules Action Users Computers	Authorized computers Only allow connections from these computers: Add Remove
	Exceptions Skip this rule for connections from these computers: Add Remove Note: computer identities can only be verified if an authentication method that carries computer identity is used.
	< Back Finish Cancel

Exercise 3: Allow Key Management Service on the Domain and Private network, and deny the connection on the Public network

A KMS is used to activate Microsoft products (such as Windows and Office) within an organization without requiring each machine to connect directly to Microsoft for activation.

1. Open the Windows Defender Firewall with Advanced Security options

Windows Security

about:blank

_	Ē	×

← ≡ ŵ Home	((۱۷) Firewall & network protection Who and what can access your networks.	Windows Community videos Learn more about Firewall & network protection
Virus & threa	t protection		
(ili) Firewall & ne	twork protection	Domain network Firewall is on.	
므 Device secur	ty F	Private network	Who's protecting me? Manage providers
	Z F	Public network (active) Firewall is on.	Change your privacy settings View and change privacy settings for your Windows 10 device. Privacy settings Privacy dashboard Privacy Statement
	r F F F	Allow an app through firewall Network and Internet troubleshooter Firewall notification settings Advanced settings Restore firewalls to default	

🔅 Settings

- 2. Scroll to the Key Management Service inbound rule in the Overview panel of Windows Defender Firewall with Advanced Security. Note the following:
- The policy is currently not enabled (the Enabled column says No.)
- If enabled, the rule would allow communication (the Action column says Allow.)

Double-click this rule.

P Windows	Defender Firewall with Advanced Security						
File Action	View Help						
💠 🔿 🖄	T B I I T						
P Windows	Defe Inbound Rules						
Inbou	ind Rules	Group	Profile	Enabled	Action	Override	Р ^
S conn	ction File and Printer Sharing over SMBDirect (i	File and Printer Sharing over	All	No	Allow	No	S
> 🔍 Monit	orinc 🔮 Google Chrome (mDNS-ln)	Google Chrome	All	Yes	Allow	No	C
	iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow	No	%
	Key Management Service (TCP-In)	Key Management Service	All	No	Allow	No	%
	🔮 mDNS (UDP-In)	mDNS	Domain	Yes	Allow	No	%
	🔮 mDNS (UDP-In)	mDNS	Private	Yes	Allow	No	%
	🔮 mDNS (UDP-In)	mDNS	Public	Yes	Allow	No	%
	Netlogon Service (NP-In)	Netlogon Service	All	No	Allow	No	S

3. Here you will see the details of this rule. You will note that the General tab includes the name of the rule, a description of the rule, and whether the rule has been allowed or blocked. In this case, the connection is allowed. Click the Advanced tab.

Key Manager	ment Service (TCP-In) Properties	×
Protocols an General	d Ports Scope Advanced Local Principals Remote U Programs and Services Remote Computers	lsers ;
	This is a predefined rule and some of its properties cannot be modified.	
	Name: Key Management Service (TCP-In) Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 16881 Enabled	
Action		
	 Allow the connection Allow the connection if it is secure Customize Block the connection 	
	OK Cancel App	ly

4. Here you will see which profiles the rule applies to. In this case, **Domain**, **Private** and **Public** are all selected.

Key Management	Service	(TCP-In)	Properties
----------------	---------	----------	------------

 \times

Gener	al	Program	s and Services		Remote	e Computers
Protocols a	and Ports	Scope	Advanced	Local	Principals	Remote Users
Profiles	Specify pr Doma Privat Public	ofiles to wh in e	ich this rule ap	plies.		
Interfac	e types					
	Specify th rule applie	e interface s.	types to which	this	Customiz	e
Edge tra	versal					
S.	Edge trav inbound p such as a firewall.	ersal allows ackets that Network A	the computer have passed t ddress Transla	to accep through tion (NA	ot unsolicite an edge de T) router or	d vice
	Block ed	ge traversa	I		~	
	Prevent a the Intern	applications let through	from receiving a NAT edge de	unsolici avice.	ted traffic fro	m
			ОК		Cancel	Apply

5. Because we want to allow communication only with the domain and private networks, For **Public** this box should not have a checkmark. Next, click **Apply**, then click **Ok**.

Key Manage	ment Ser	vice (TCP-	In) Properties				×
General		Program	s and Services		Remote	e Computers	
Protocols ar	nd Ports	Scope	Advanced	Local	Principals	Remote Users	5
	Specify p Doma Privat Privat	rofiles to wh ain te c	ich this rule apş	olies.			
Interface	types	_					
	Specify th rule applie	ne interface es.	types to which	this	Customiz	:e	
Edge trav	versal						
S.	Edge trav inbound p such as a firewall.	versal allows backets that Network A	the computer t have passed t ddress Translat	o acce; hrough ion (NA	ot unsolicited an edge dev T) router or	d vice	
	Block ed	lge traversa	I		~		
	Prevent the Inter	applications net through	from receiving a NAT edge de	unsolici vice.	ted traffic fro	om	
			OK		Cancel	Apply	

6. Next, right click on Key Management Service(TCP-In) and select Enable Rule.

iSCSI Service (TCP-	-In)	iSCSI Service	All	No	Allow
Key Management	Service (TCP-In)	Key Management Service	All	No	Allow
🔮 mDNS (UDP-Ir	Enable Rule	mDNS	Private	Yes	Allow
🔮 mDNS (UDP-Ir	Cut	mDNS	Domain	Yes	Allow
🔮 mDNS (UDP-Ir	Carrie	mDNS	Public	Yes	Allow
🥑 Microsoft Edge	Сору	Microsoft Edge	All	Yes	Allow
🥑 Microsoft Med	Delete	Microsoft Media Foundatio	All	Yes	Allow
🥑 Microsoft Med	Properties	Microsoft Media Foundatio	All	Yes	Allow
Netlogon Servi		Netlogon Service	All	No	Allow
Netlogon Servi	Help	Netlogon Service	All	No	Allow
		·			

This will be set as Yes which means now the communication with the domain and private network is allowed.

11	iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
	🦉 Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
11.4	(al-BOU) 200	2MDm	Drivate	Vec	Allow

7. Now we will create an inbound rule that blocks communication with the public network. Since the new rule will be similar to the last, we will copy the existing rule. Right-click the Key Management Service (TCP-In) inbound rule and click Copy. Press Ctrl+V to paste.



about:blank

8. You will now see a second Key Management Service (TCP-In) inbound rule. Double-click the second rule to open the Key Management Service TCP-IN) Properties.

ISCSI SERVICE (TCP-III)	1903L SELVICE	All	INO	Allow
😵 Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
🧶 Key Management Service (TCP-In)	Key Management Service	All	Yes	Allow
🚺 mDNS (LIDP-In) 🛌	2MDm	Public	Ves	Allow

9. Since we want to block connection with the public network, select Block the connection on the General tab. Click Apply.

otocols a	nd Ports	Scope	Advanced	Local Pr	incipals	Remote U
Genera		Program	s and Services	1	Remote	e Computers
i	This is a p be modifie	oredefined i ed.	rule and some	of its prope	rties canr	not
General						
	Name:					
-	Key Mana	agement Se	ervice (TCP-In)			
	Description	n:				
	Inbound r	ule for the	Key Manageme	ent Service	to allow	^
	16881	ne counting	g and license c	ompliance		~
	Enable	ed				
<i>.</i>	Allow t Allow t Cust Block	the connect the connect tomize	tion tion if it is secu ction	re		

10. Click the Advanced tab.

General Programs and Services Remote Computers Image: Computers This is a predefined rule and some of its properties cannot be modified. General Image: Computers Image: Computers Name: Computers Image: Computers Computers Image: Comput	Protocols a	nd Ports	Scope	Advanced	Local Principals	Remote User
 (i) This is a predefined rule and some of its properties cannot be modified. General Name: Key Management Service (TCP-In) Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 1688] Enabled Action Allow the connection Allow the connection if it is secure Customize (index the connection) 	Genera		Program	s and Services	Remot	e Computers
General Image: Name: Marcina Control Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 16881 Image:	()	This is a be modifi	predefined ed.	rule and some o	of its properties cann	not
Name: Imagement Service (TCP-In) Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 1688] Action Imagement Service (TCP-In) Allow the connection Imagement Service (TCP-In) Imagement Service (TCP-In) <td>General</td> <td></td> <td></td> <td></td> <td></td> <td></td>	General					
 Key Management Service (TCP-In) Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 16881 Enabled Action Allow the connection Allow the connection if it is secure Customize Block the connection 		Name:				
Description: Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 16881 Center Constant of the connection Allow the connection if it is secure Customize I Block the connection		Key Man	agement Se	ervice (TCP-In)		
Inbound rule for the Key Management Service to allow for machine counting and license compliance. [TCP 16881 Action Allow the connection Allow the connection if it is secure Customize Block the connection		Descriptio	n:			20
Action Allow the connection Allow the connection Customize Block the connection		Inbound	ule for the	Key Manageme	ent Service to allow	^
Action Allow the connection Allow the connection if it is secure Customize Block the connection		16881	ne counting	g and license ci	ompliance. [ICP	~
Action Allow the connection Allow the connection if it is secure Customize Isolate the connection 		Enabl	ed			
Action Allow the connection Allow the connection if it is secure Customize Block the connection	Action					
 Allow the connection if it is secure Customize Block the connection 	Action		the conner	tion		
Customize Block the connection	1		the connect	tion if it is secu	re	
 Block the connection 						
 Block the connection 		Cus	tomize			
		Block	the conne	ction		

11. Click the **Domain** and **Private** boxes to remove the checkmarks. Click the **Public** to add the checkmark. Click **Ok**.

Key Management Service (TCP-In) Properties	×
General Programs and Services Remote Compute Protocols and Ports Scope Advanced Local Principals Remote	ers Users
Profiles Specify profiles to which this rule applies. Domain Private V Public	
Interface types	
Specify the interface types to which this rule applies.	
Edge traversal	
Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device such as a Network Address Translation (NAT) router or firewall.	
Block edge traversal \sim	
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.	
OK Cancel A	pply

12. The Overview panel will show your changes. Right-click each Key Management Service (TCP-In) rule and click Enable rule.

Key Management Service (TCP-In)	Key Managemen	Domain, Private
Key Management Service (TCP-In)	Key Managemen	Public

13. Now you will see that a green checkmark appears next to the first rule indicating that the rule allowing communication is enabled. A circle with a line through it appears next to the second rule indicating that the rule blocking communication is enabled.

Inbound Rules					
Name	Group	Profile	Enabled	Action	^
Key Management Service (TCP-In)	Key Managemen	Domain, Private	Yes	Allow	
Key Management Service (TCP-In)	Key Managemen	Public	Yes	Block	

Author(s)

Dee Dee Collette

© IBM Corporation. All rights reserved.