Chapter 6

Hardening and Security

Page 281 (Chapter 7) - Mastering-Windows-Server-2016

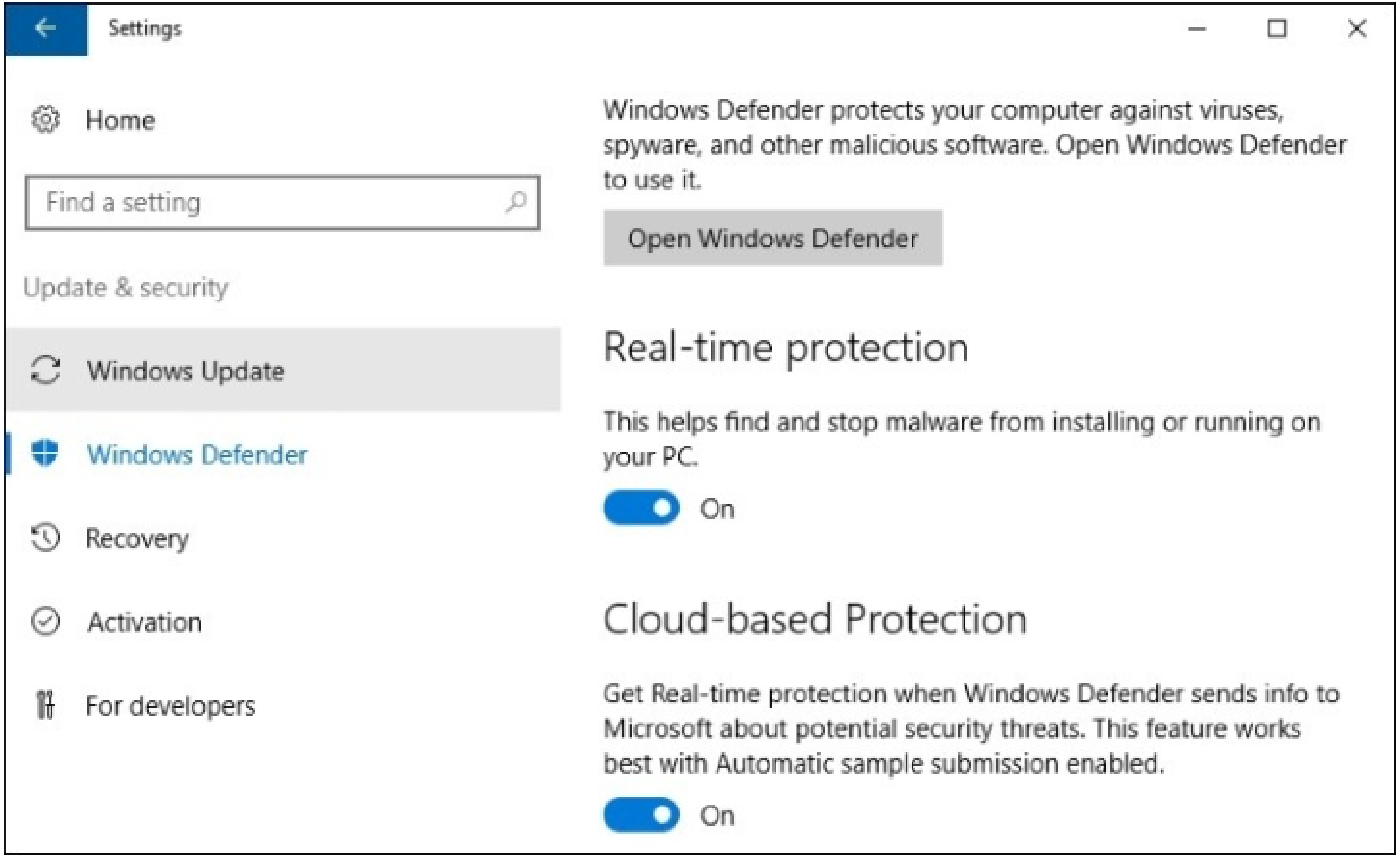
Windows Defender

Installing Windows Defender

Windows Defender is installed by default in Windows Server 2016. However, the graphical user interface may not be available, depending on what specific SKU of Server 2016 you have installed. If you do not see a configuration console for Windows Defender, you can easily add the Windows Defender feature either from the Add Roles and Features wizard, or by using this PowerShell cmdlet:

```
Install-WindowsFeature –Name Windows-Defender-GUI
```

Windows Defender



Windows Defender protects your computer against viruses, spyware, and other malicious software. Open Windows Defender to use it.

Open Windows Defender

Real-time protection

This helps find and stop malware from installing or running on your PC.

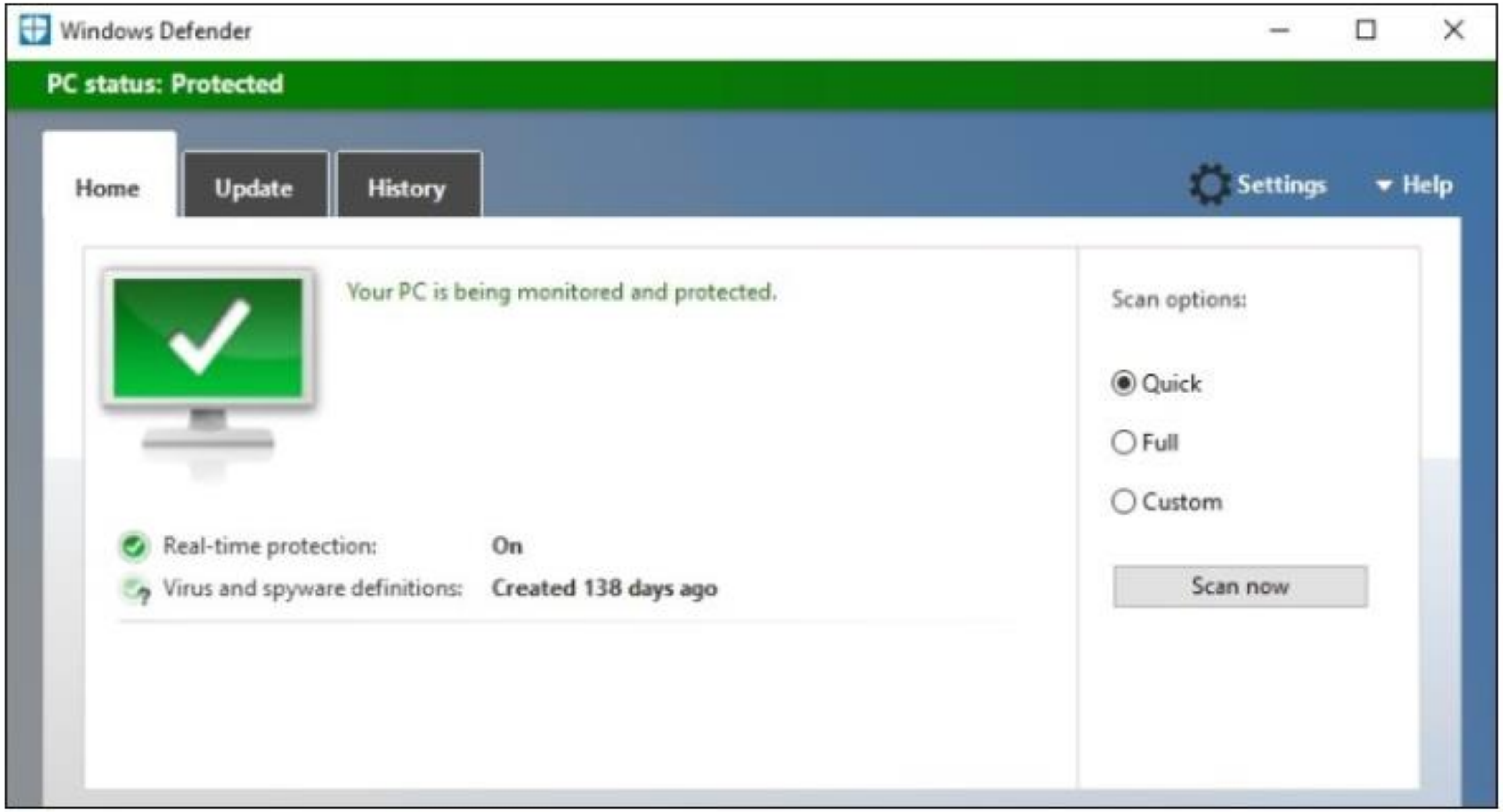
On

Cloud-based Protection

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

On

Windows Defender



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Created 138 days ago

Scan options:

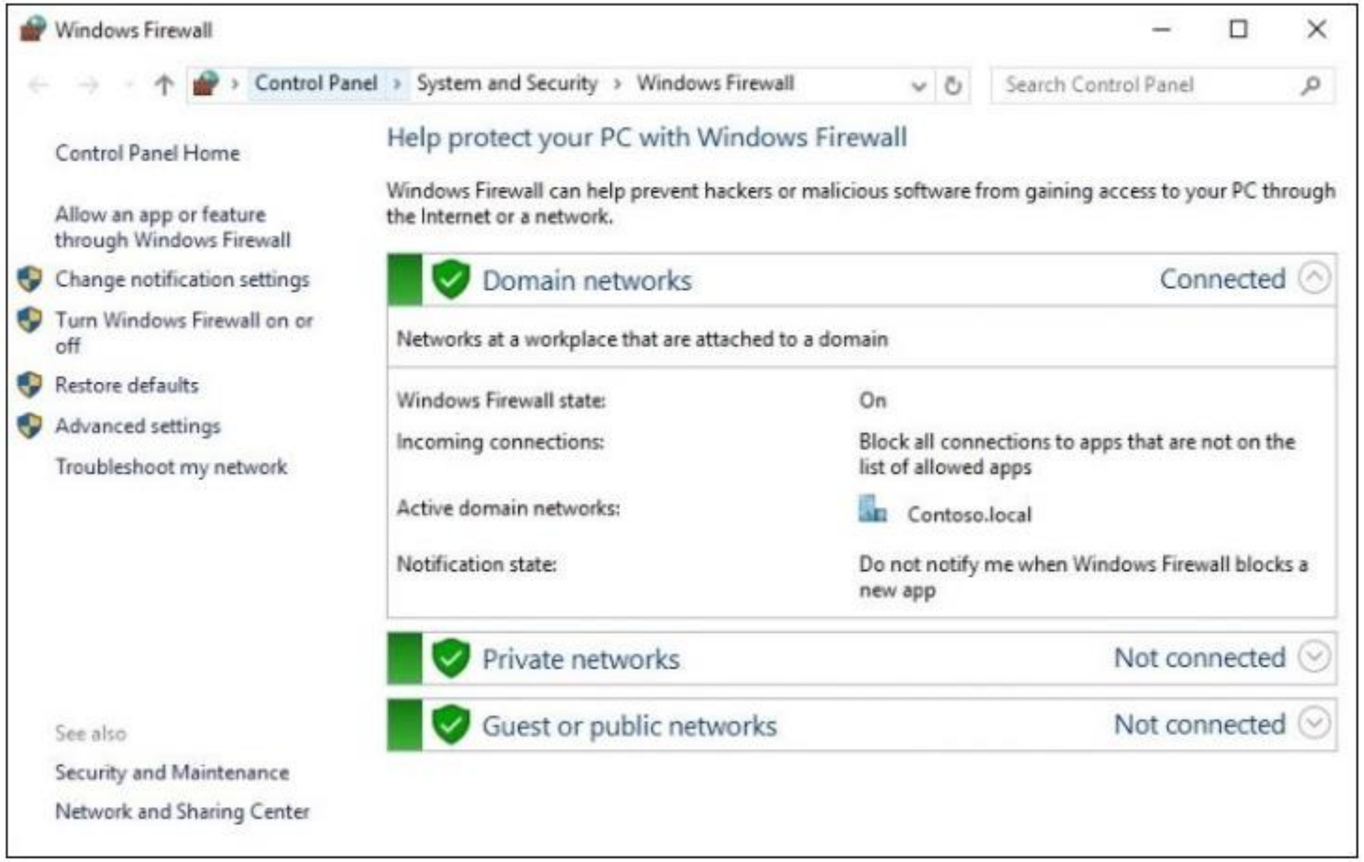
● Quick

○ Full

○ Custom

Windows Firewall

Windows Firewall settings



Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

Networks at a workplace that are attached to a domain

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

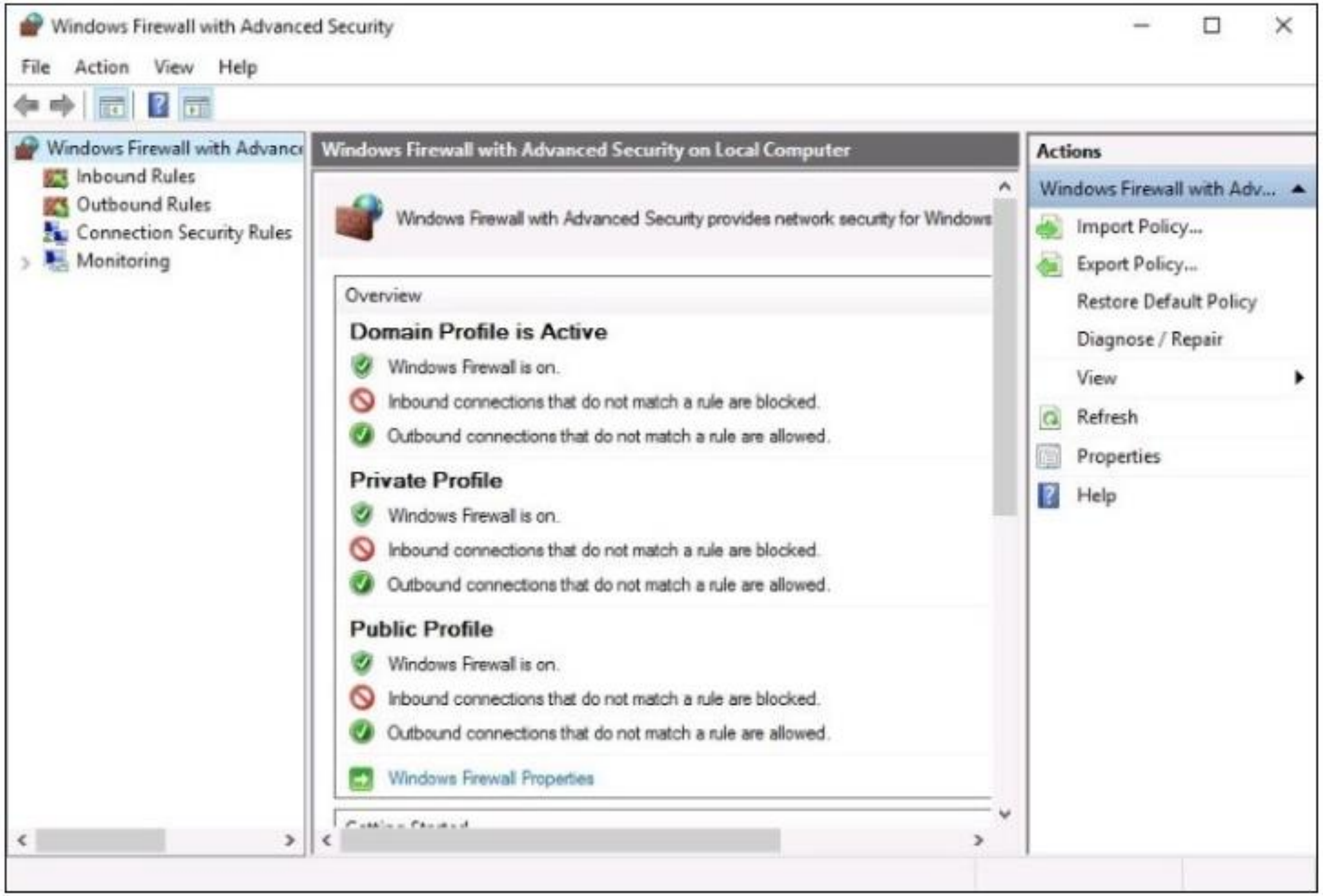
Active domain networks: Contoso.local

Notification state: Do not notify me when Windows Firewall blocks a new app

Private networks — Not connected

Guest or public networks — Not connected

Windows Firewall



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows

Overview

Domain Profile is Active

- ✓ Windows 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 Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

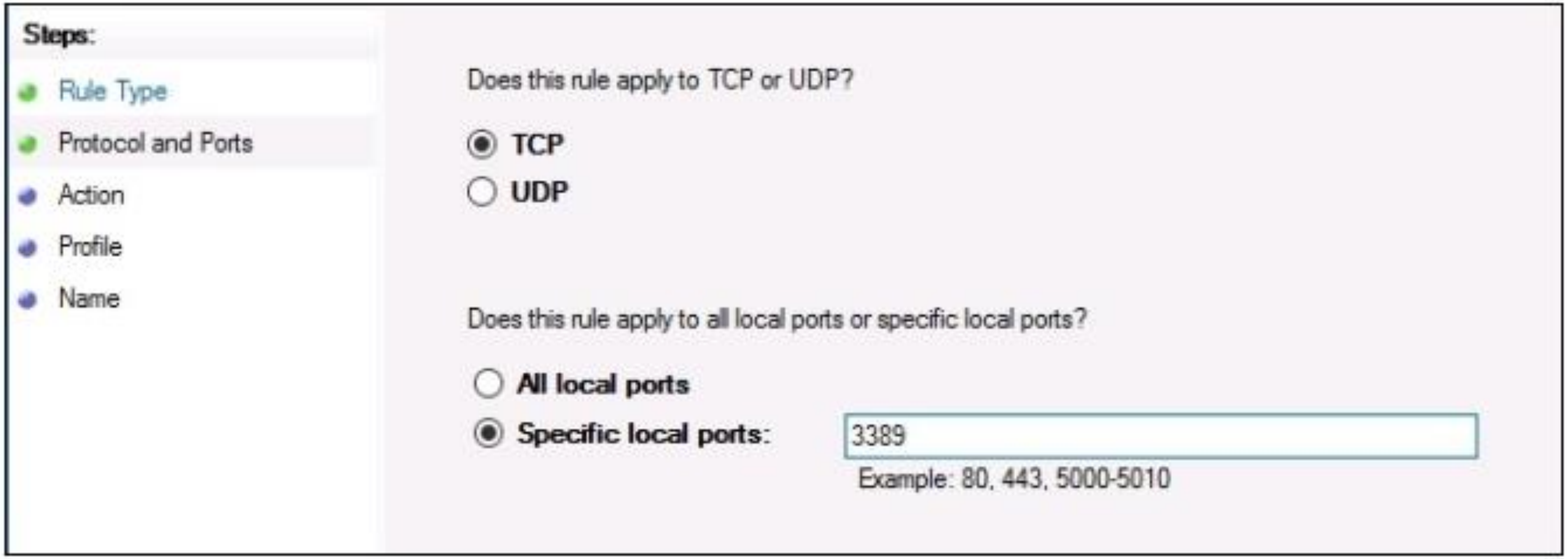
Public Profile

- ✓ Windows Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Windows Firewall

Building a new Inbound Rule



Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

Does this rule apply to all local ports or specific local ports?

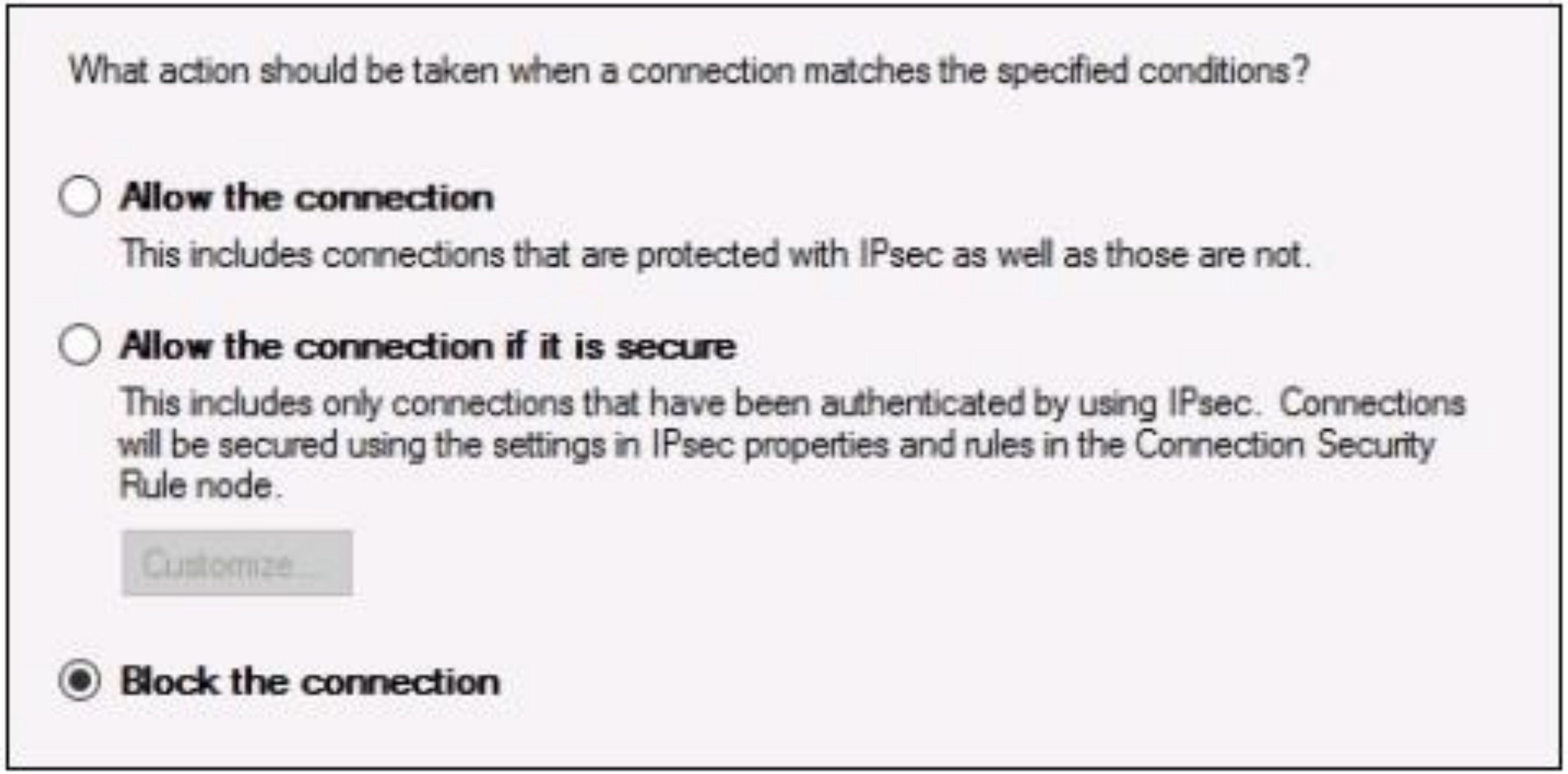
○ All local ports

● Specific local ports: 3389

Example: 80, 443, 5000-5010

Windows Firewall

Building a new Inbound Rule



What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

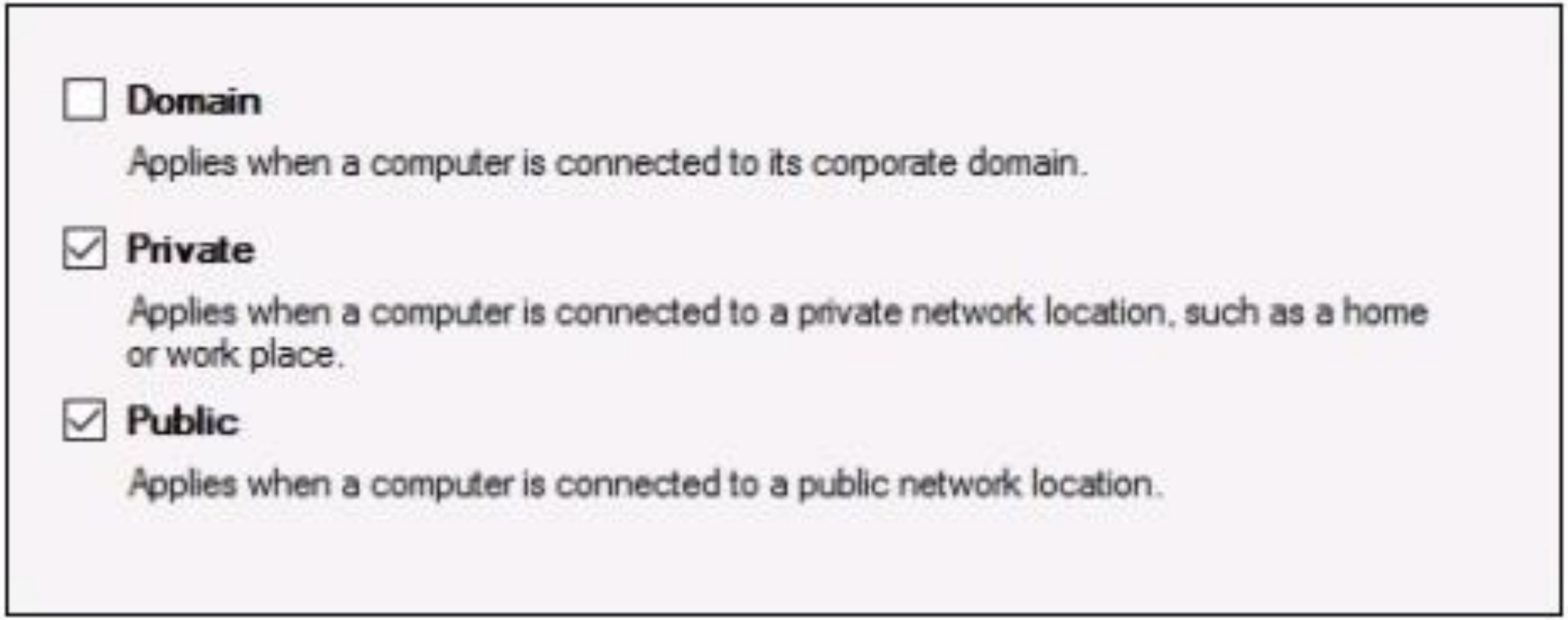
○ **Allow the connection if it is secure**

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 Rule node.

● **Block the connection**

Windows Firewall

Building a new Inbound Rule



□ **Domain**

Applies when a computer is connected to its corporate domain.

☑ **Private**

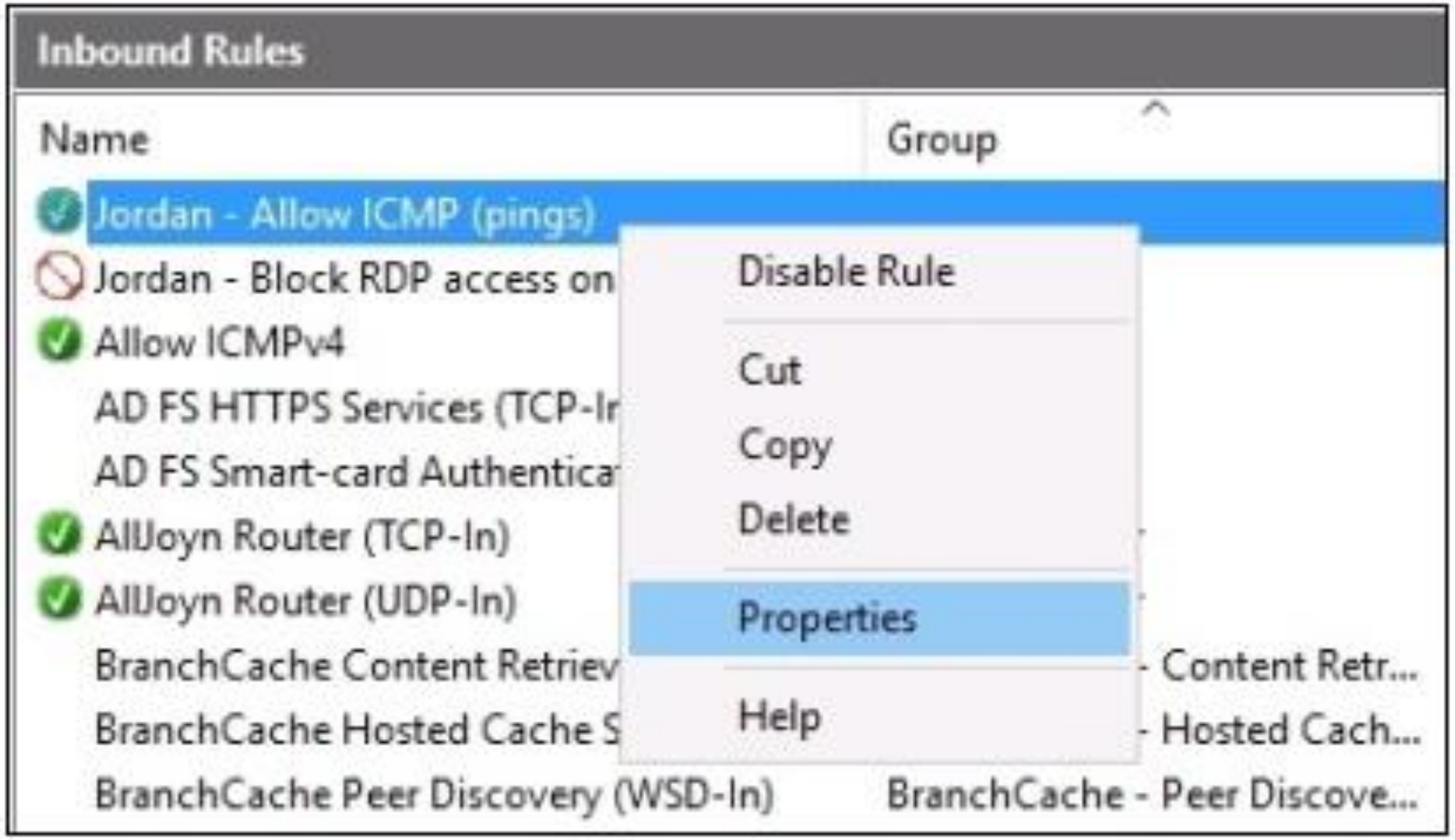
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**

Applies when a computer is connected to a public network location.

Windows Firewall

Ex: build a rule for ICMP

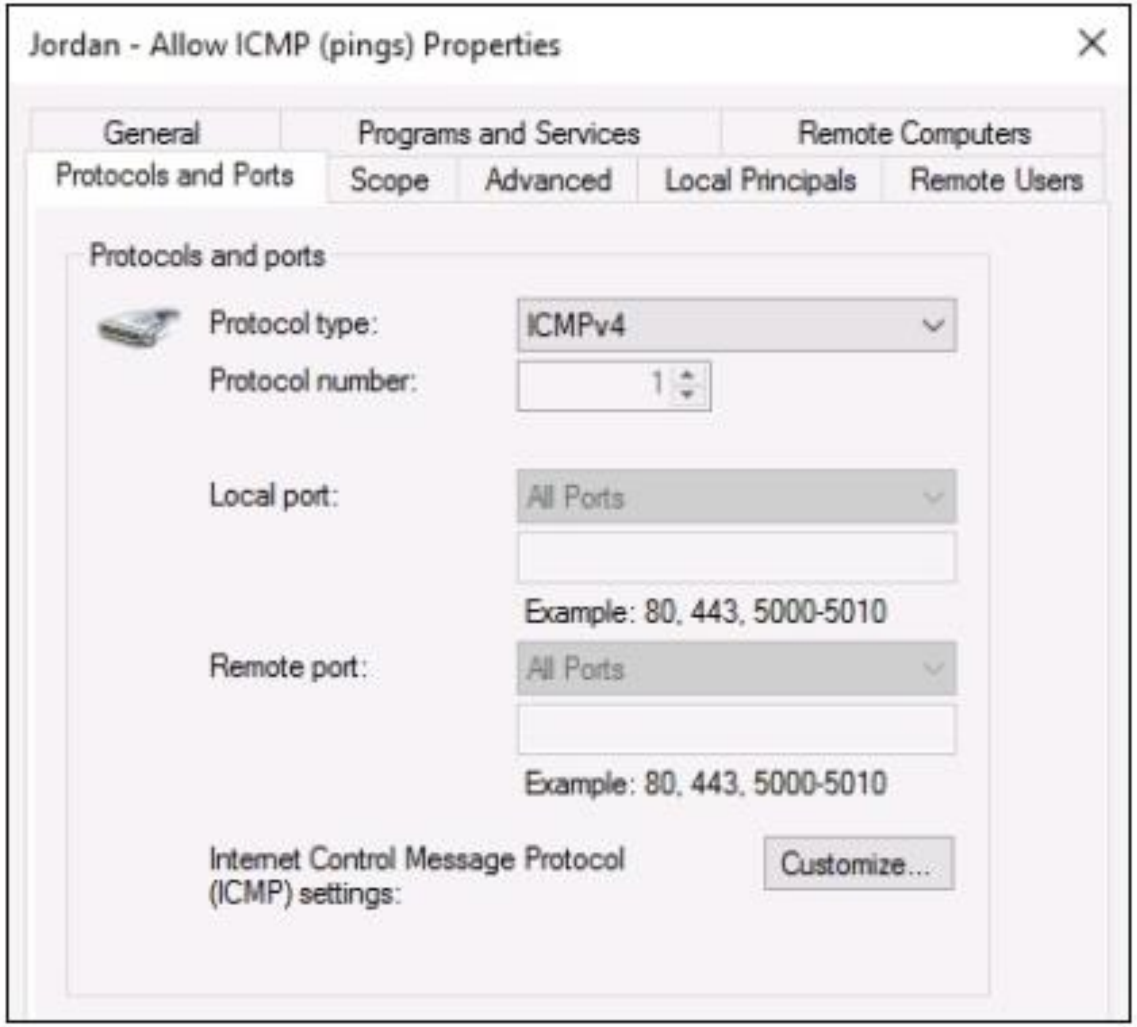


Inbound Rules

Name	Group
✓ Jordan - Allow ICMP (pings)	
⃠ Jordan - Block RDP access on	
✓ Allow ICMPv4	
AD FS HTTPS Services (TCP-Ir	
AD FS Smart-card Authentica	
✓ AllJoyn Router (TCP-In)	
✓ AllJoyn Router (UDP-In)	
BranchCache Content Retriev	- Content Retr...
BranchCache Hosted Cache S	- Hosted Cach...
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...

Windows Firewall

Ex: build a rule for ICMP



Jordan - Allow ICMP (pings) Properties

Protocols and ports

Protocol type: ICMPv4

Protocol number: 1

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

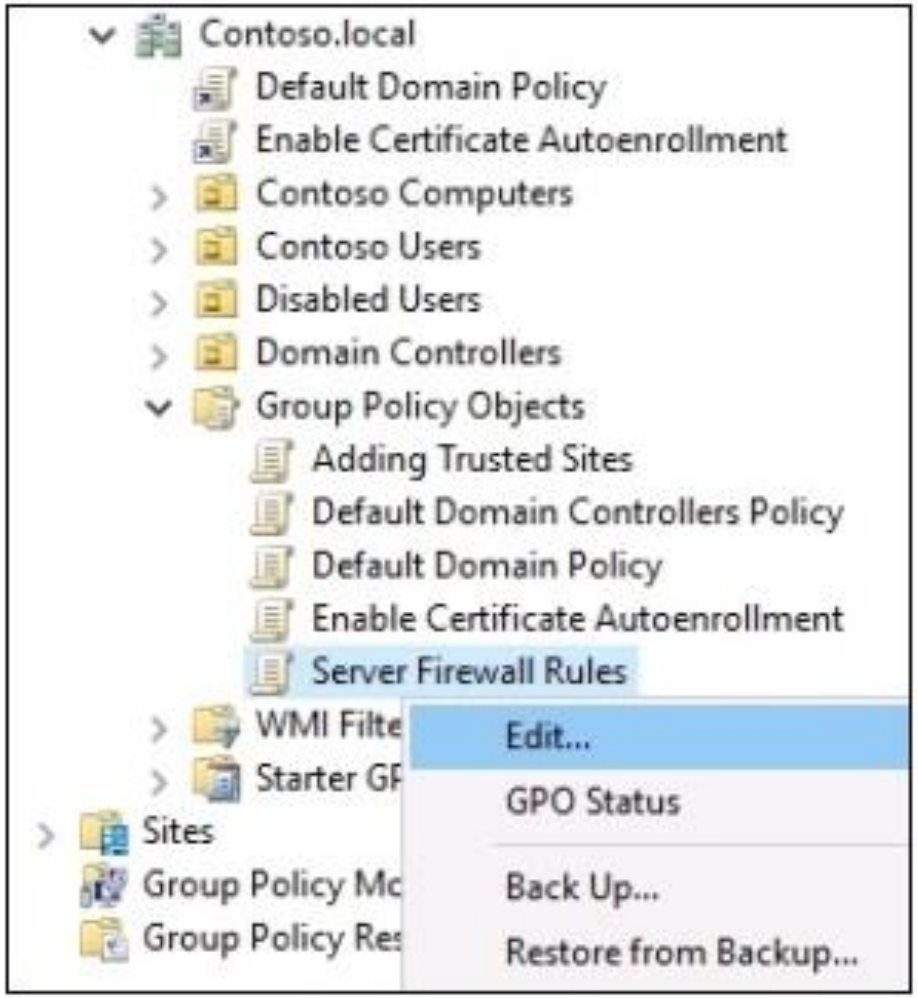
Windows Firewall

Managing WFAS with Group Policy

Managing firewall rules on your servers, and clients, can be a huge step toward a more secure environment for your company. The best part? This technology is enterprise class, and free to use since it's already built into the operating systems that you use. The only cost you have associated with firewalling at this level is the time it takes to put all of these rules into place, which would be an administrative nightmare if you had to implement your entire list of allows and blocks on every machine individually.

Windows Firewall

Managing WFAS with Group Policy



Contoso.local
- Default Domain Policy
- Enable Certificate Autoenrollment
- Contoso Computers
- Contoso Users
- Disabled Users
- Domain Controllers
- Group Policy Objects
  - Adding Trusted Sites
  - Default Domain Controllers Policy
  - Default Domain Policy
  - Enable Certificate Autoenrollment
  - Server Firewall Rules
- WMI Filte
- Starter GF

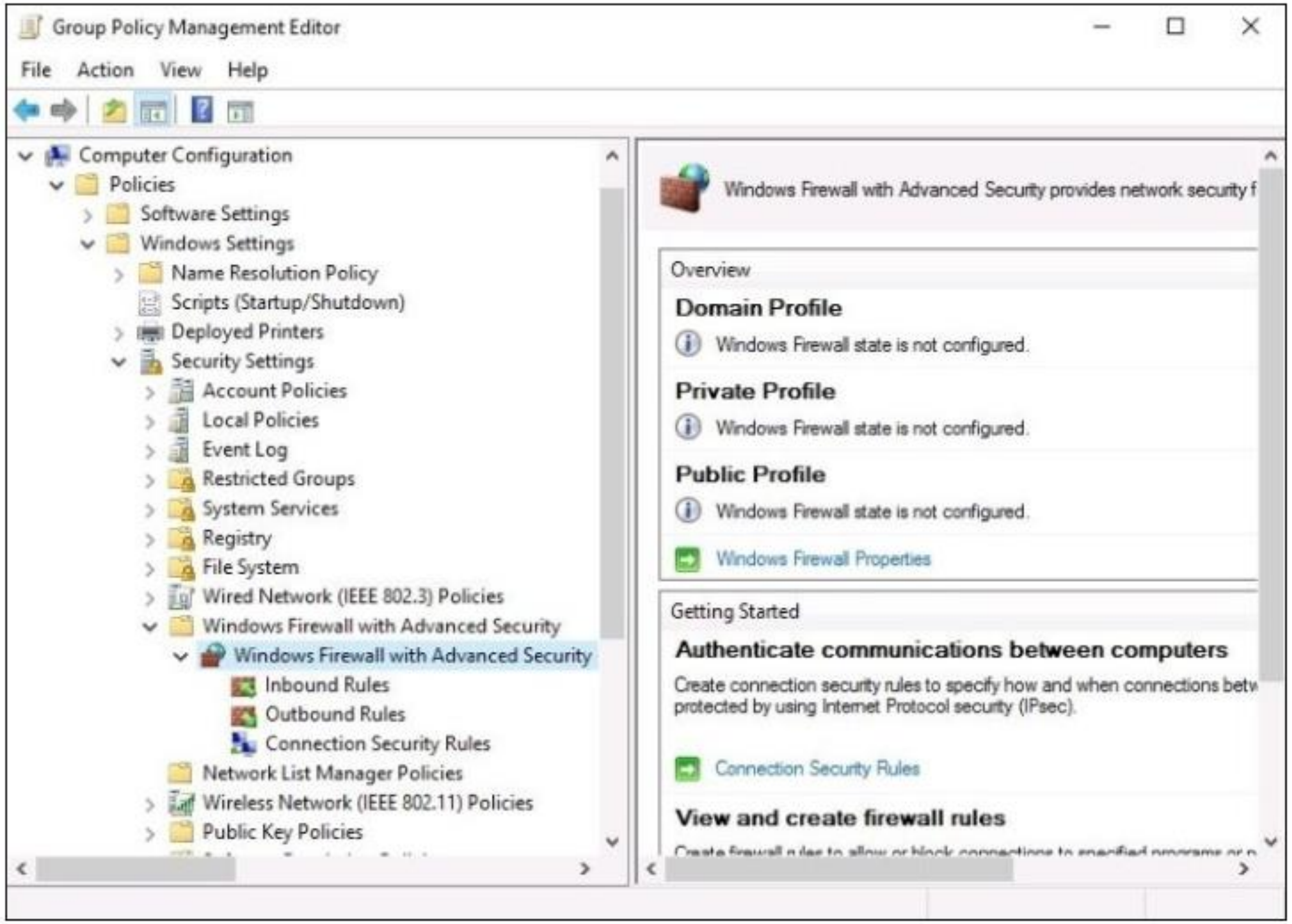
Sites

Group Policy Mc

Group Policy Res

Windows Firewall

Managing WFAS with Group Policy



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
          - Windows Firewall with Advanced Security
            - Inbound Rules
            - Outbound Rules
            - Connection Security Rules
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies

Windows Firewall with Advanced Security provides network security f

Overview

Domain Profile

Windows Firewall state is not configured.

Private Profile

Windows Firewall state is not configured.

Public Profile

Windows Firewall state is not configured.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections betw protected by using Internet Protocol security (IPsec).

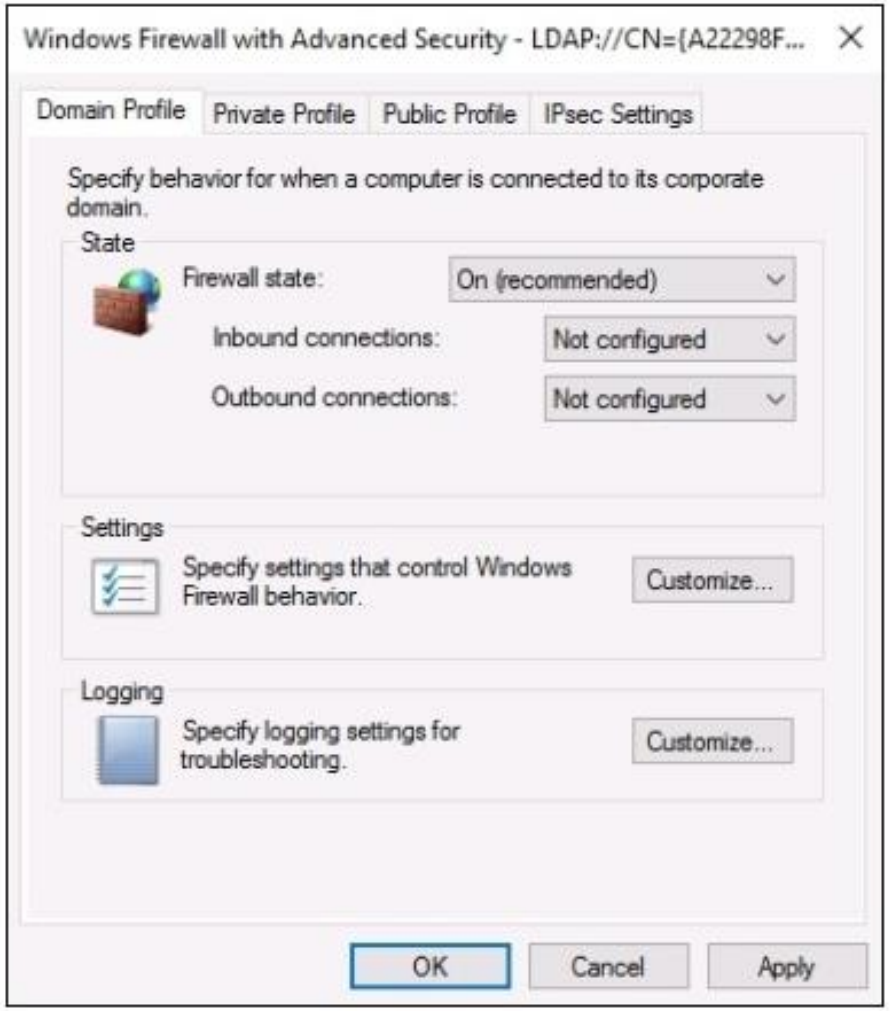
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or p

Windows Firewall

Managing WFAS with Group Policy



Windows Firewall with Advanced Security - LDAP://CN={A22298F...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Not configured

Outbound connections: Not configured

Settings

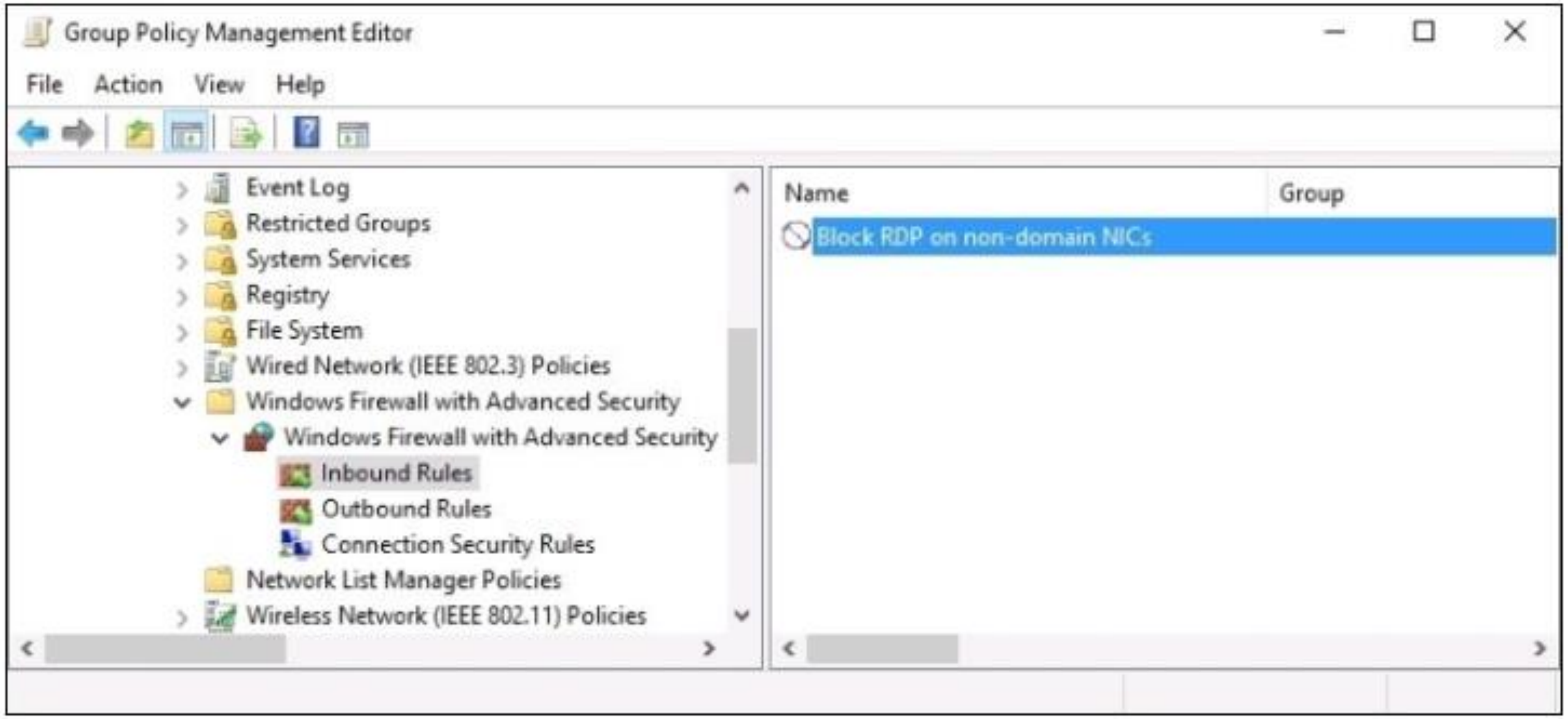
Specify settings that control Windows Firewall behavior.

Logging

Specify logging settings for troubleshooting.

Windows Firewall

Managing WFAS with Group Policy



Group Policy Management Editor
File
Action
View
Help
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Name
Group

Block RDP on non-domain NICs

Q & A