[illegible] WFAS [illegible] Group Policy [illegible] 2019 [illegible]

[illegible] ICMP [illegible]. [illegible] ICMP [illegible]. [illegible] RDP [illegible].

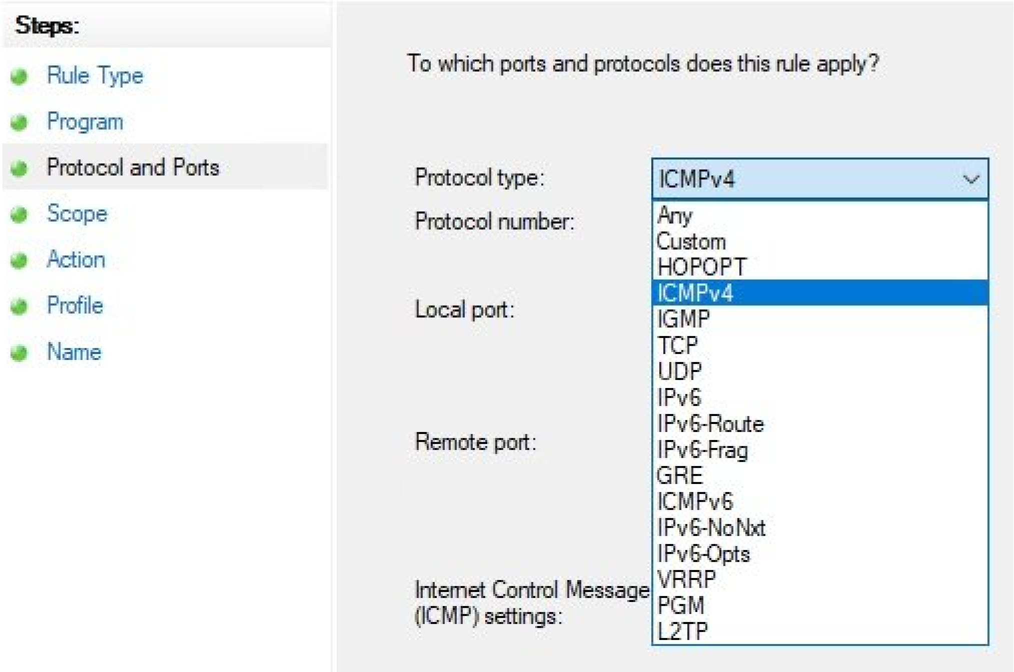
[illegible] [illegible] 2019 [illegible] [illegible].

[illegible] ICMP [illegible]

[illegible] ICMP [illegible]. [illegible] RDP [illegible]. [illegible] Rule Type [illegible]

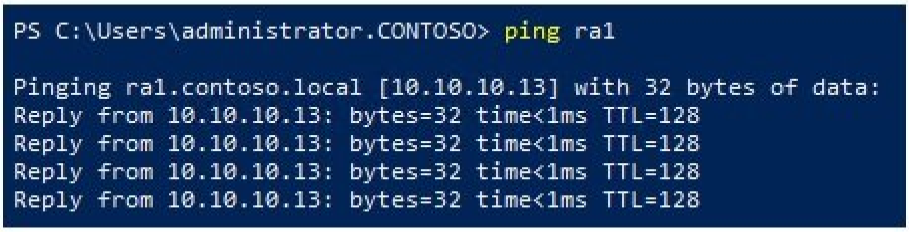
[illegible] ICMP [illegible]. [illegible] ICMP [illegible]. [illegible] RDP [illegible] Custom [illegible].

[illegible] All programs [illegible] Next [illegible]. [illegible] ICMP [illegible]. [illegible] ICMPv4 [illegible] ICMPv6 [illegible]. [illegible] ICMPv4 [illegible].



Protocol type: ICMPv4

[illegible] RDP [illegible]. [illegible] Allow [illegible]. [illegible] ICMPv4 [illegible] Allow [illegible]:

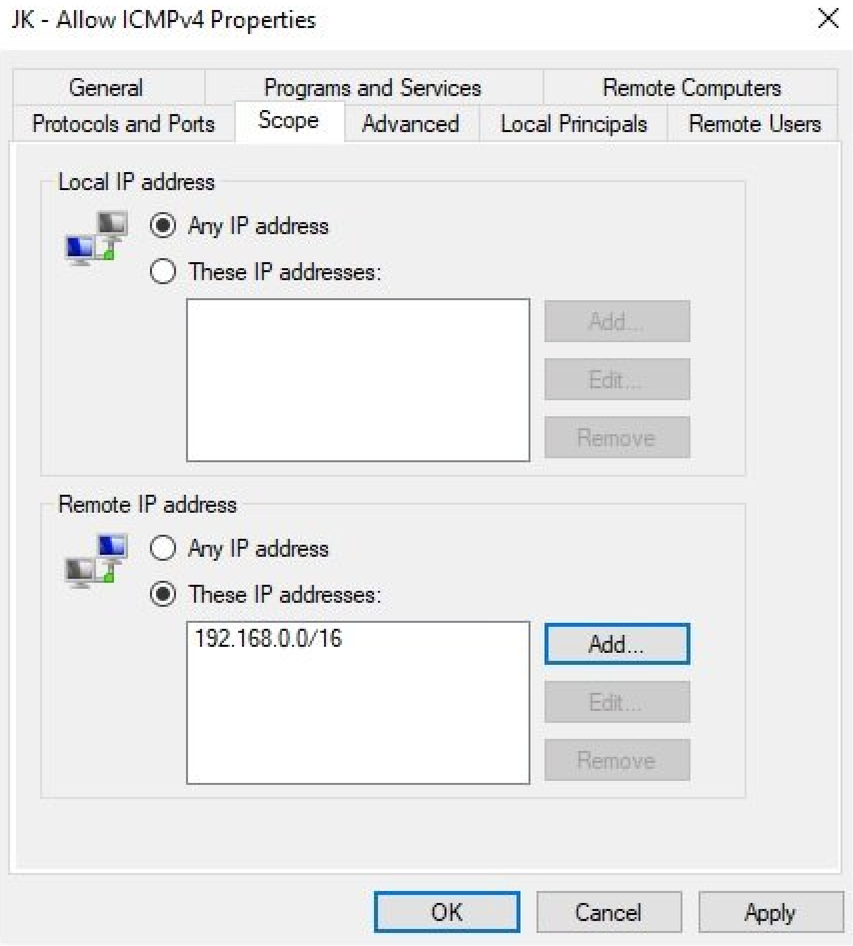


```
PS C:\Users\administrator.CONTOSO> ping ra1

Pinging ra1.contoso.local [10.10.10.13] with 32 bytes of data:
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
```

[illegible] Inbound Rules [illegible] Properties [illegible]. [illegible] Scope [illegible].

[illegible] Scope [illegible]. [illegible] 192.168.0.0/16 [illegible]:


JK - Allow ICMPv4 Properties

Local IP address: ● Any IP address

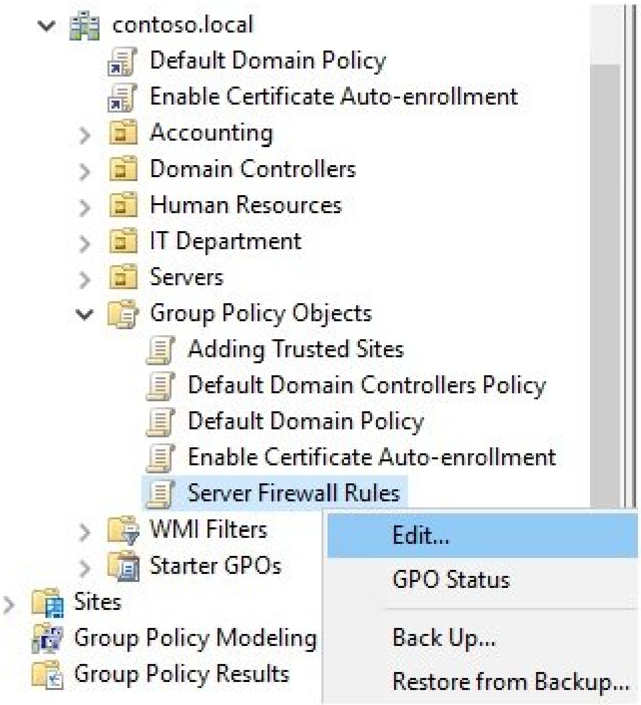
Remote IP address: ● These IP addresses: 192.168.0.0/16

[illegible] WFAS [illegible] Group Policy

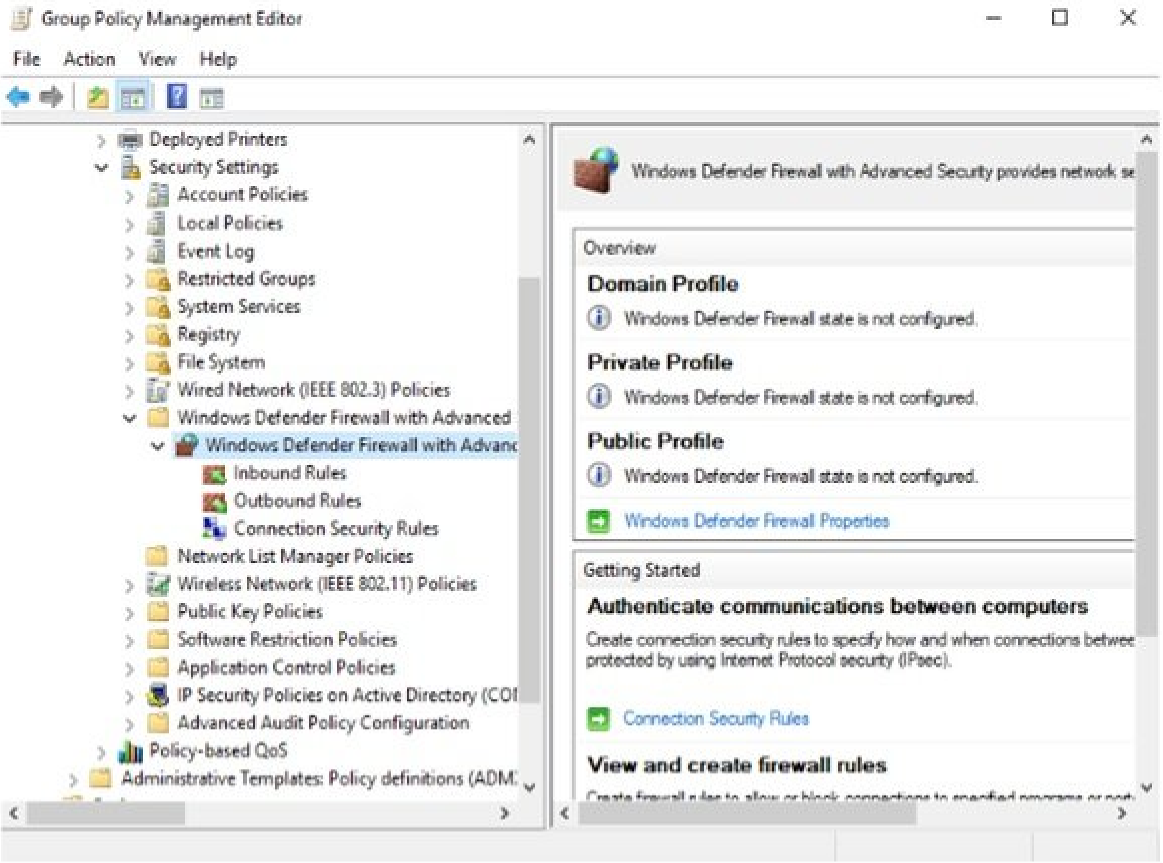
[illegible].

[illegible] (GPO) [illegible] Group Policy Object [illegible]. [illegible] GPO [illegible] GPO [illegible] GPO [illegible] GPO [illegible].

[illegible] GPO [illegible] GPO [illegible] GPO [illegible]. [illegible] OU [illegible] GPO [illegible]. [illegible] GPO [illegible] Group Policy Management Console [illegible] Edit ... [illegible]:



[illegible] GPO [illegible]. [illegible] Windows Defender Firewall with Advanced Security [illegible] Computer Configuration | Policies | Windows Settings | Security Settings | Windows Defender Firewall with Advanced Security | Windows Defender Firewall with Advanced Security [illegible].


Group Policy Management Editor
File
Action
View
Help
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced
Windows Defender Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (CO
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Overview
Domain Profile
Private Profile
Public Profile
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Connection Security Rules
View and create firewall rules

Windows Defender Firewall with Advanced Security provides network se

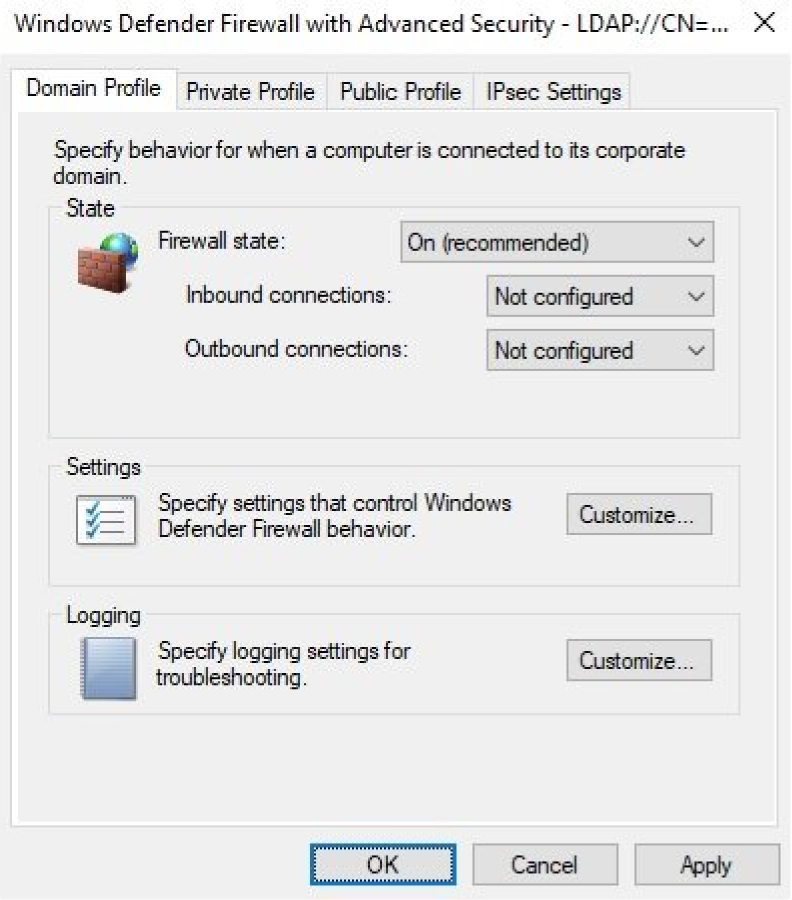
Domain Profile: Windows Defender Firewall state is not configured.

Private Profile: Windows Defender Firewall state is not configured.

Public Profile: Windows Defender Firewall state is not configured.

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

[illegible]. [illegible] Windows Defender Firewall، [illegible].


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

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

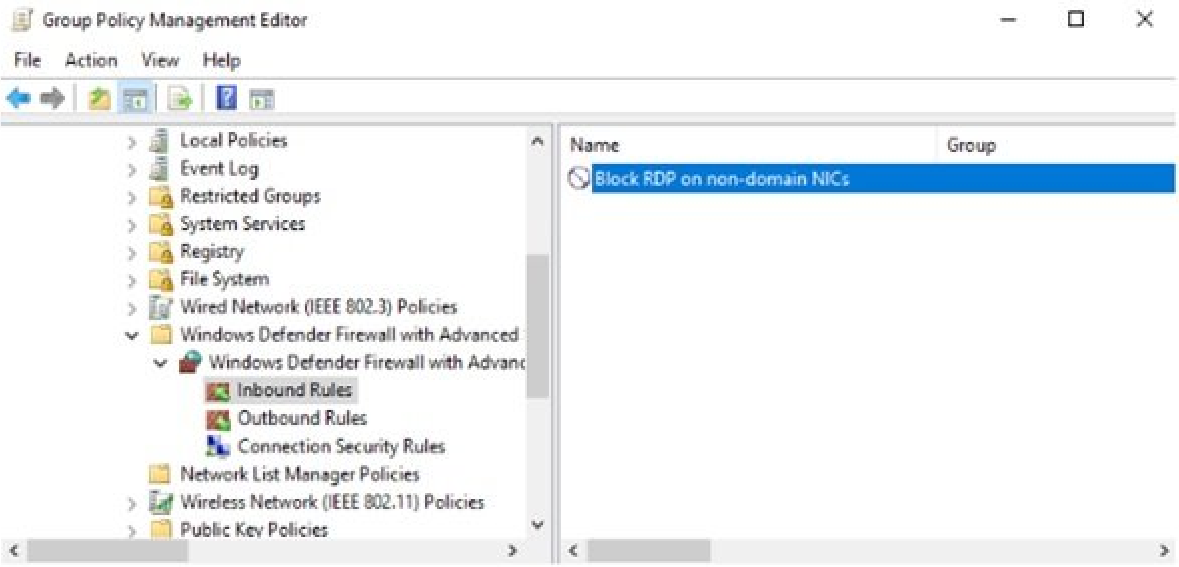
Settings

Specify settings that control Windows Defender Firewall behavior.

Logging

Specify logging settings for troubleshooting.

[illegible] ok [illegible] WFAS [illegible] GPO [illegible]. [illegible] WFAS، [illegible]. [illegible] Inbound Rules [illegible] New Rule [illegible]. [illegible] WFAS [illegible] GPO [illegible]. [illegible].


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

Block RDP on non-domain NICs

[illegible] [illegible]

[illegible] HTTPS [illegible] HTTP [illegible] HTTP [illegible]

[illegible] 2019 [illegible]

BitLocker [illegible] TPM [illegible]

BitLocker [illegible]

[illegible]

(VMs) [illegible] VHD [illegible] VHDX [illegible] VHDX [illegible].

[illegible] 2019 [illegible].

[illegible] **2019** [illegible]:

[illegible] 2019

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
18:45 - 25/08/1398
[illegible]:
[illegible] 2019 - [illegible] 2019 - Windows Server 2019 - [illegible] 2019 - [illegible] 2019 - Advanced Threat Analytics - [illegible] 2019 - Encryption - Windows Defender Firewall - Windows Defender Advanced Threat Protection - technologies - [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/networking-technology/16265/%D9%85%D8%AF%DB%8C%D8%B1%DB%8C%D8%AA-wfas-%D8%A7%D8%B2-%D8%B7%D8%B1%DB%8C%D9%82-group-policy-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019