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

[illegible] ICMP [illegible]. [illegible]

[illegible] 2019 [illegible].

[illegible] ICMP [illegible]

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

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
ICMPv4
Protocol number:
Any
Custom
HOPOPT
ICMPv4
IGMP
TCP
UDP
IPv6
IPv6-Route
IPv6-Frag
GRE
ICMPv6
IPv6-NoNxt
IPv6-Opts
VRRP
PGM
L2TP
Local port:
Remote port:
Internet Control Message (ICMP) settings:

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

این قابلیت به شما این امکان را میدهد تا قاعده دیوارآتش خود را فقط در ارتباط با ترافیک یا بخش خاصی از شبکه یا یک زیر مجموعه خاص از ماشینها اعمال کنید . به عنوان مثال، در اینجا من زبانه Scope را ویرایش کردم تا قاعده جدی تنها روی ترافیکی که از زیرشبکه 192.168.0.0/16 وارد میشود اعمال شود :

JK - Allow ICMPv4 Properties

Local IP address
● Any IP address
○ These IP addresses:

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

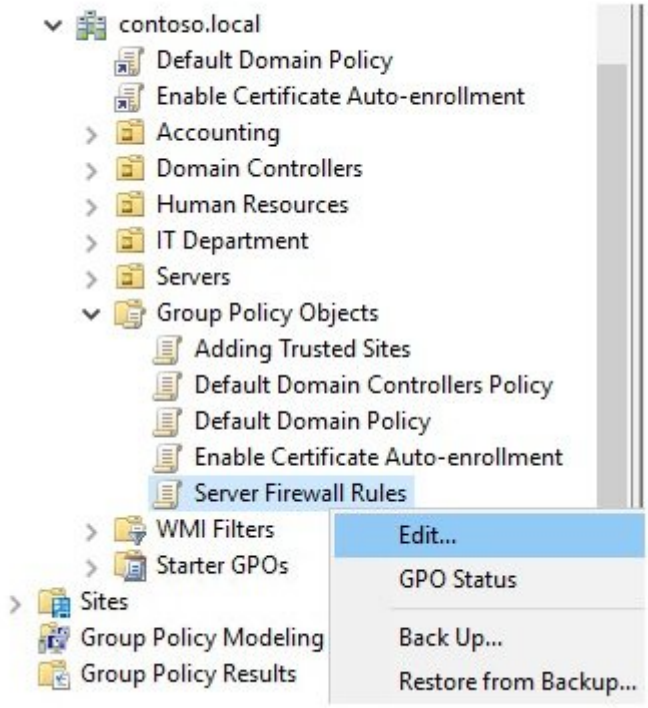
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Add...
Edit...
Remove
Add...
Edit...
Remove
OK
Cancel
Apply

مدیریت WFAS از طریق Group Policy

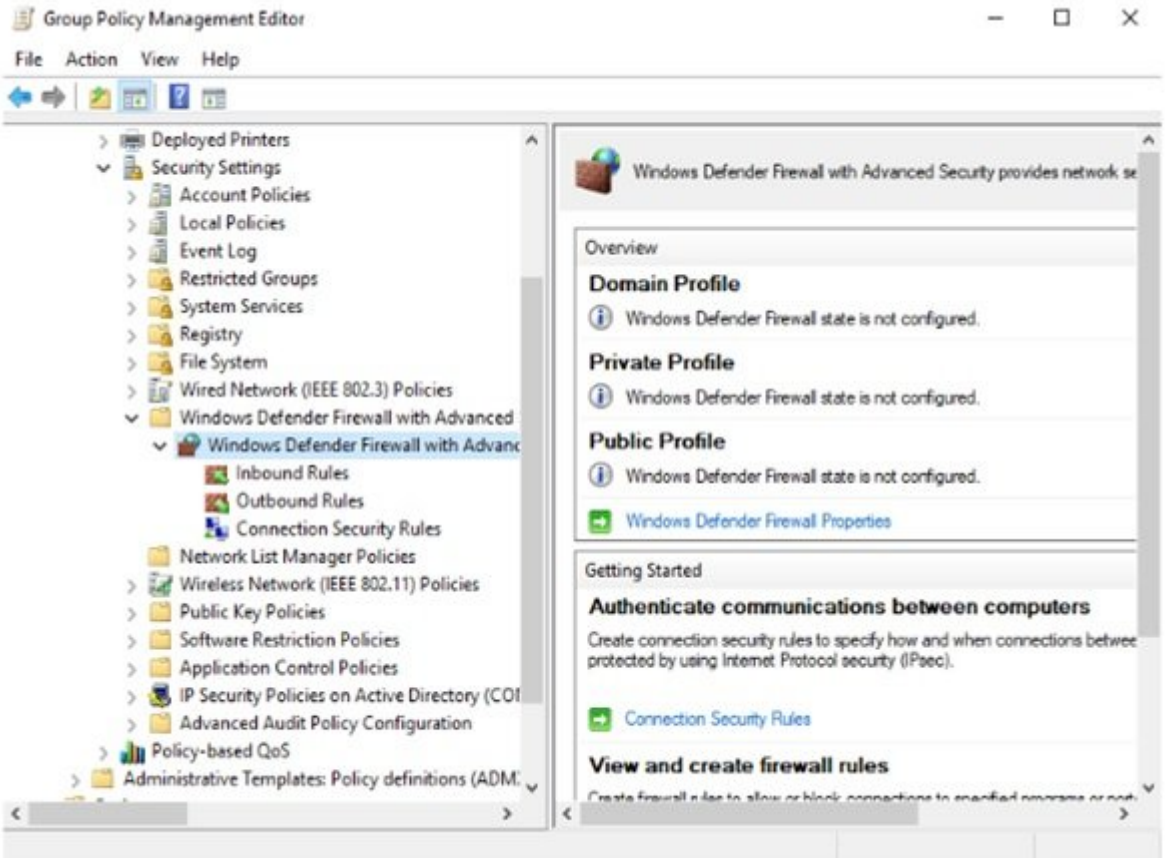
مدیریت قواعد دیوارآتش روی سرورها و کلاینتها میتواند گامی بزرگ در جهت ایجاد یک محیط امنتر باشد. لازم به توضیح است که فناوری فوق در کلاس سازمانی است، در نتیجه مایکروسافت تمهیداتی در نظر گرفته تا اگر قرار است یک قاعده روی ماشینهای خاصی اعمال شود، کارشناسان مجبور نشوند یک به یک به سراغ ماشینها بروند و یک قاعده خاص را روی آنها اعمال کنند .

برای حل این مشکل باید از راهکار خطمشی گروهی (GPO) سرنام Group Policy Object استفاده کنید . همانند اکثر تنظیمات و عملکردهای موجود در سیستمعامل ویندوز مایکروسافت، تنظیم یک خطمشی دیوارآتش روی همه دستگاههایی که متصل به دامنه هستند اعمال میشود. البته شما میتوانید خطمشیهای خود را به چند مجموعه تقسیم کنید تا یک GPO تنها روی کلاینتها اعمال شود، در حالی که یک GPO جداگانه قواعد دیوارآتش را روی سرورها اعمال کند . نکتهای که لازم است به آن دقت کنید این است که شما میتوانید ماشینها را گروهبندی کنید و برای هر گروه مجموعه قوانین GPO ایجاد کنید و بهطور خودکار قاعده ساخته شده را در ارتباط با ماشینهایی که عضو یک GPO هستند اعمال کنید .

شما قبلاً با نحوه ساخت GPO آشنا شدهاید، بنابراین یک GPO که قرار است تنظیمات دیوارآتش را شامل شود ایجاد کنید . GPO را لینک کرده و فیلتر کنید تا فقط دستگاههای مدنظر تنظیمات را دریافت کنند . شاید ایده بدی نباشد که فرآیند فوق را با OU آزمایش کنید تا اطمینان حاصل کنید تمام قواعدی که میخواهید داخل GPO قرار دهید به خوبی در کنار هم قرار گرفتند و با خطمشیهای امنیتی سازمان سازگار باشند . پس از ایجاد GPO جدید، از داخل Console Management Policy Group روی آن راست کلیک کنید و سپس Edit ... را انتخاب کنید :



.Computer Configuration | Policies | Windows Settings | Security Settings | Windows Defender Firewall with Advanced Security | Windows Defender Firewall with Advanced Security



Windows Defender Firewall with Advanced Security - LDAP://CN=...
Domain Profile
Private Profile
Public Profile
IPsec Settings
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.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
OK
Cancel
Apply

[illegible]

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

[illegible] **2019** [illegible]

[illegible] TPM [illegible] BitLocker

BitLocker [illegible]

(VMs) ماشین های مجازی ساخته شده در نسخه های قبلی ویندوز سرور فقط از فرمت VHD پشتیبانی می کردند. اما در ویندوز سرور 2019 فرمت جدیدی به نام VHDX به وجود آمده است که دارای ویژگی های بسیار بیشتری نسبت به فرمت VHD است. از جمله این ویژگی ها می توان به پشتیبانی از حجم های بزرگتر، مقاومت بیشتر در برابر خرابی و بهبود عملکرد اشاره کرد. اگر شما از ماشین های مجازی استفاده می کنید، حتما پیشنهاد می کنیم که از فرمت VHDX استفاده کنید. برای تبدیل فرمت VHD به VHDX می توانید از ابزار Convert-VHD در PowerShell استفاده کنید. این ابزار به شما امکان می دهد که فرمت فایل های VHD را به VHDX تبدیل کنید.

در ادامه مطالب آموزشی مجموعه شبکه 2019 را مشاهده می کنید.

در ادامه مطالب آموزشی مجموعه **2019** را مشاهده می کنید:

2019 مجموعه آموزشی ویندوز سرور

:نویسنده
مجموعه آموزشی
:تاریخ انتشار
مجموعه آموزشی
:آخرین بروزرسانی
18:45 - 25/08/1398
:برچسب
2019 مجموعه آموزشی ویندوز سرور - Windows Server 2019 - 2019 مجموعه آموزشی ویندوز سرور - 2019 مجموعه آموزشی ویندوز سرور - 2019 مجموعه آموزشی مدیریت ویندوز سرور - Advanced Threat Analytics - 2019 مجموعه آموزشی ویندوز سرور - Windows Defender Advanced Threat Protection - Windows Defender Firewall - Encryption technologies - مجموعه آموزشی فناوری

منبع:
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