

WCI 341

The Windows Vista Firewall with IPsec

Don't connect without it!

Filtering directions

Inbound

Default:
Block most
Few core exceptions

Allow rules:
Programs, services
Users, computers
Protocols, ports

Outbound

Default:
Allow all interactive
Restrict services

Block rules:
Programs, services
Users, computers
Protocols, ports



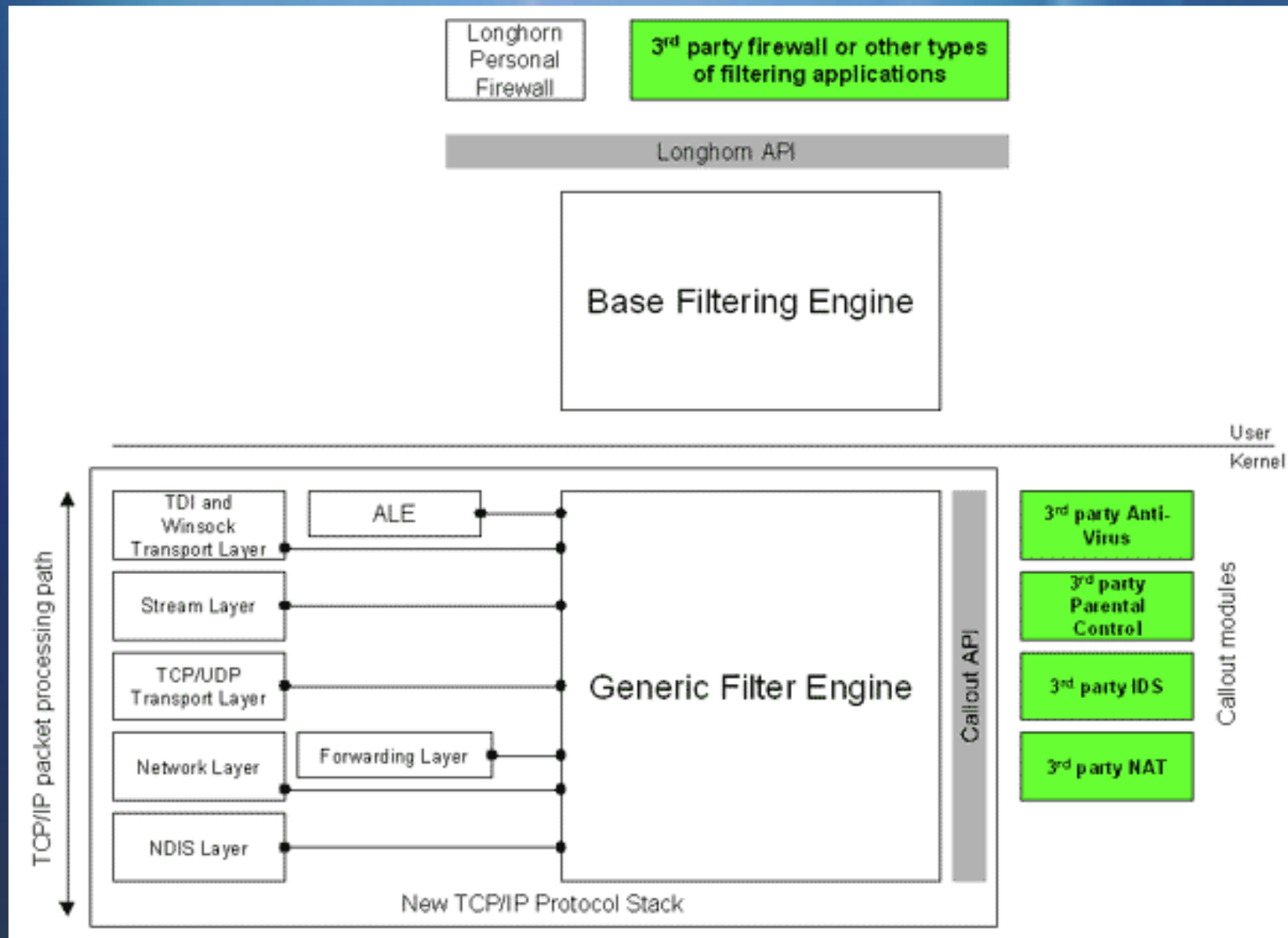
Comparing features

	Windows XP SP2	Windows Vista
<i>Direction</i>	Inbound	Inbound, outbound
<i>Default action</i>	Block	Configurable for direction
<i>Packet types</i>	TCP, UDP, some	All
<i>Rule types</i>	Application, global ports, ICMP types	Multiple conditions from basic five-tuple to IPsec metadata
<i>Rule actions</i>	Block	Block, allow, bypass; with rule merge logic
<i>UI and tools</i>	Control Panel, netsh	C-Panel, more netsh, MMC
<i>APIs</i>	Public COM, private C	More COM to expose rules, more C to expose features
<i>Remote management</i>	none	Via hardened RPC interface
<i>Group policy</i>	ADM file	MMC, netsh
<i>Terminology</i>	Exceptions; profiles	Rules; categories=profiles

Windows filtering platform

- Series of APIs for 3rd-party products to hook into stack to make filtering decisions at various layers
- Provides next-generation filtering features
 - Authenticated communication
 - Dynamic firewall configuration based on WinSock calls
 - Foundation for Windows Firewall and IPsec
 - Works with encrypted traffic
 - Which is much more prevalent in Vista; e.g., RPC
- Stack hooking now fully documented
 - No need to build custom filtering logic
 - Little risk that conforming apps will break after service pack release

WFP architecture



Architecture improvements

- API calls are synchronous
 - Rule is guaranteed to be applied if call returns success
- User context is available
 - Audits of policy changes show user context
- ACLs are in the API calls in the service
 - No registry ACLs now
 - No more escalation of privilege
- Policy updates are incremental

Configuration

- Control panel: similar to Windows XP
 - A few changes to presentation
- New MMC user interface for all the extra goodies
 - “Windows Firewall with Advanced Security” snap-in
 - Predefined console in Administrative Tools
 - Can assign settings to remote computers
 - Integrates *and simplifies* IPsec settings here, too
- Also new `netsh advfirewall` command line

Rule types

<i>Program</i>	Allows traffic for a particular program
<i>Port</i>	Allows traffic on a particular TCP or UDP port or list of ports
<i>Predefined</i>	Groups of rules that allow Windows functionality on the network (for instance: file and printer sharing, network discovery, remote assistance, remote service administration, Windows collaboration, others)
<i>Custom</i>	All the knobs and dials, switches and buttons

The firewall rule

```
DO Action = {By-pass | Allow | Block} IF:  
  Protocol = X AND  
  Direction = {In | Out} AND  
  Local TCP/UDP port is in {Port list} AND  
  Remote TCP/UDP port is in {Port list} AND  
  ICMP type code is in {ICMP type-code list} AND  
  Interface NIC is in {Interface ID list} AND  
  Interface type is in {Interface types list} AND  
  Local address is found in {Address list} AND  
  Remote address is found in {Address list} AND  
  Application = <Path> AND  
  Service SID = <Service Short Name> AND  
  Require authentication = {TRUE | FALSE} AND  
  Require encryption = {TRUE | FALSE} AND  
  Remote user has access in {SDDL} AND  
  Remote computer has access in {SDDL} AND  
  OS version is in {Platform List}
```

Example rules

Allow Internet Explorer to connect outbound to destination port 80/tcp

Allow svchost.exe hosting RPCSS to listen for inbound traffic on port 135/tcp from remote addresses

Allow UPnP service to listen for inbound traffic on *<Interface-ID>* from USB devices, on ports 2869 and 1900 (must use API for rules with *<interface-ID>*s)

Block svchost.exe hosting MPSSVC from connecting outbound or listening inbound

Allow svchost.exe hosting PolicyAgent to listen on dynamic RPC ports from remote computer *<hostname>* and user *<username>*

Rule merging and evaluation order

High
st



Low
st

Service restrictions

Restricts connections that services can establish; OS services already configured appropriately

Connection rules

Restricts connections from particular computers; uses IPsec to require authentication and authorization

Authenticated bypass

Allows specified authenticated computers to bypass other rules

Block rules

Explicitly blocks specified incoming or outgoing traffic

Allow rules

Explicitly allows specified incoming or outgoing traffic

Default rules

Default behavior for a connection

CAUTION

Rules are stored in registry.

Editing rules directly in the registry is UNSUPPORTED and will usually result in severe pain, undefined behavior, loss of all friends, and general ridicule on the newsgroups

Default rules

Registry Editor

File Edit View Favorites Help

- RemoteAccess
- RemoteRegistry
- RFCOMM
- RpcLocator
- RpcSs
- rsndr
- SamSs
- sb2port
- SCardSrv
- Collab-P2PHost-In-TCP
- Schedule
- SCPolicySvc
- sdbus
- SDRSVC
- secdrv
- seconlog
- SENS
- Serenum
- Serial
- sermouse
- ServiceModelEndpoint 3.0.0.0
- ServiceModelOperation 3.0.0.0
- ServiceModelService 3.0.0.0
- SessionEnv
- sfidisk
- sfpp_mmc
- sfpp_sd
- sloppy
- SharedAccess
- Defaults
 - FirewallPolicy
 - DomainProfile
 - Logging
 - FirewallRules
 - PublicProfile
 - Logging
 - StandardProfile
 - Logging
 - Epoch
 - Parameters
 - ShellHWDetection
 - sisapp
 - SiSRaid2
 - SiSRaid4
 - sluvc
 - SLUINotify
 - Smb
 - SMSvcHost 3.0.0.0
 - smwmd
 - SNMPTRAP
 - spldr
 - Spooler
 - srv
 - srv2
 - srndet
 - SDSPSRV
 - stsvc
 - swenum
 - swprv
 - Sym_hi
 - Sym_u3
 - Sym_u3

Name	Type	Data
[Default]	REG_SZ	(value not set)
BITSSVC-In-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=6 Port=2178 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28262 Desc=@FirewallAPI.dll,-28265 EmbedCtxt=@FirewallAPI.dll,-28254 Desc=@FirewallAPI.dll,-28254
BITSSVC-In-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=17 Port=3702 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28262 Desc=@FirewallAPI.dll,-28265 EmbedCtxt=@FirewallAPI.dll,-28254 Desc=@FirewallAPI.dll,-28254
BITSSVC-Out-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=6 Port=2178 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28266 Desc=@FirewallAPI.dll,-28269 EmbedCtxt=@FirewallAPI.dll,-28258 Desc=@FirewallAPI.dll,-28258
BITSSVC-Out-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=17 Port=3702 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28266 Desc=@FirewallAPI.dll,-28269 EmbedCtxt=@FirewallAPI.dll,-28258 Desc=@FirewallAPI.dll,-28258
BITSSVC-RPC-In-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=6 Port=RPC RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28270 Desc=@FirewallAPI.dll,-28270 EmbedCtxt=@FirewallAPI.dll,-28270 Desc=@FirewallAPI.dll,-28270
BITSSVC-RPCSS-In-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=6 Port=RPC-EPMap RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-28274 Desc=@FirewallAPI.dll,-28274 EmbedCtxt=@FirewallAPI.dll,-28274 Desc=@FirewallAPI.dll,-28274
Collab-P2PHost-In-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=6 App=System Name=@FirewallAPI.dll,-32003 Desc=@FirewallAPI.dll,-32006 EmbedCtxt=@FirewallAPI.dll,-32002 Desc=@FirewallAPI.dll,-32002
Collab-P2PHost-Out-TCP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=6 App=System Name=@FirewallAPI.dll,-32007 Desc=@FirewallAPI.dll,-32010 EmbedCtxt=@FirewallAPI.dll,-32002 Desc=@FirewallAPI.dll,-32002
Collab-P2PHost-WSD-In-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=17 Port=3702 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-32011 Desc=@FirewallAPI.dll,-32011 EmbedCtxt=@FirewallAPI.dll,-32011 Desc=@FirewallAPI.dll,-32011
Collab-P2PHost-WSD-Out-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=17 Port=3702 RA4=LocalSubnet RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-32011 Desc=@FirewallAPI.dll,-32011 EmbedCtxt=@FirewallAPI.dll,-32011 Desc=@FirewallAPI.dll,-32011
Collab-PNRP-In-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=17 Port=3540 App=System Name=@FirewallAPI.dll,-32019 Desc=@FirewallAPI.dll,-32022 EmbedCtxt=@FirewallAPI.dll,-32022 Desc=@FirewallAPI.dll,-32022
Collab-PNRP-Out-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=17 Port=3540 App=System Name=@FirewallAPI.dll,-32023 Desc=@FirewallAPI.dll,-32026 EmbedCtxt=@FirewallAPI.dll,-32026 Desc=@FirewallAPI.dll,-32026
Collab-PNRP-SSDP-Srv-In-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=In Protocol=17 Port=1900 App=System Name=@FirewallAPI.dll,-32031 Desc=@FirewallAPI.dll,-32034 EmbedCtxt=@FirewallAPI.dll,-32034 Desc=@FirewallAPI.dll,-32034
Collab-PNRP-SSDP-Srv-Out-UDP	REG_SZ	v2.0>Action=Allow Active=FALSE Dir=Out Protocol=17 Port=1900 App=System Name=@FirewallAPI.dll,-32031 Desc=@FirewallAPI.dll,-32034 EmbedCtxt=@FirewallAPI.dll,-32034 Desc=@FirewallAPI.dll,-32034
CoreNet-DHCP-In	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=In Protocol=17 Port=68 App=System Name=@FirewallAPI.dll,-25301 Desc=@FirewallAPI.dll,-25303 EmbedCtxt=@FirewallAPI.dll,-25303 Desc=@FirewallAPI.dll,-25303
CoreNet-DHCP-Out	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=17 Port=68 App=System Name=@FirewallAPI.dll,-25302 Desc=@FirewallAPI.dll,-25305 EmbedCtxt=@FirewallAPI.dll,-25305 Desc=@FirewallAPI.dll,-25305
CoreNet-DNS-Out-UDP	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=17 Port=53 App=System Name=@FirewallAPI.dll,-25401 Desc=@FirewallAPI.dll,-25405 EmbedCtxt=@FirewallAPI.dll,-25405 Desc=@FirewallAPI.dll,-25405
CoreNet-GP-NP-UDP-TCP	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=6 Profile=Domain Port=445 App=System Name=@FirewallAPI.dll,-25401 Desc=@FirewallAPI.dll,-25401 EmbedCtxt=@FirewallAPI.dll,-25400 AutoGenPsec=FALSE Edge=FALSE
CoreNet-GP-Out-TCP	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=6 Profile=Domain App=System Name=@FirewallAPI.dll,-25403 Desc=@FirewallAPI.dll,-25404 EmbedCtxt=@FirewallAPI.dll,-25404 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP4-DUFRAG-In	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=In Protocol=1 ICMP4=34 App=System Name=@FirewallAPI.dll,-25251 Desc=@FirewallAPI.dll,-25257 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP4-DUFRAG-Out	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=1 ICMP4=34 App=System Name=@FirewallAPI.dll,-25252 Desc=@FirewallAPI.dll,-25257 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-DU-In	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=In Protocol=58 ICMP6=1 App=System Name=@FirewallAPI.dll,-25110 Desc=@FirewallAPI.dll,-25112 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-DU-Out	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=58 ICMP6=1 App=System Name=@FirewallAPI.dll,-25111 Desc=@FirewallAPI.dll,-25112 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-LD-In	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=In Protocol=58 ICMP6=132 RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-25082 Desc=@FirewallAPI.dll,-25088 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-LD-Out	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=58 ICMP6=132 RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-25083 Desc=@FirewallAPI.dll,-25088 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-LQ-In	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=In Protocol=58 ICMP6=130 RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-25061 Desc=@FirewallAPI.dll,-25067 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGenPsec=FALSE Edge=FALSE
CoreNet-ICMP6-LQ-Out	REG_SZ	v2.0>Action=Allow Active=TRUE Dir=Out Protocol=58 ICMP6=130 RA6=LocalSubnet App=System Name=@FirewallAPI.dll,-25062 Desc=@FirewallAPI.dll,-25067 EmbedCtxt=@FirewallAPI.dll,-25000 AutoGen

Service restriction rules

The screenshot displays the Windows Registry Editor with the following structure:

- Left pane: Tree view showing the path **Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Static\System**.
- Right pane: A table listing the registry values for these rules.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AVEndpointBuilder-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=AudioEndpointBuilder Name=Block any inbound traffic to AudioEndpointBuilder
BFE-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=BFE Name=Block inbound traffic to BFE
BFE-2	REG_SZ	V2.0 Action=Block Dir=out App=%SystemRoot%\system32\svchost.exe Svc=BFE Name=Block outbound traffic from BFE
clr_optimization_v2.0.50727_32-1	REG_SZ	V2.0 Action=Block Dir=in App=C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe Svc=clr_optimization_v2.0.50727_32 Name=Block traffic for clr_optimization_v2.0.50727_32
clr_optimization_v2.0.50727_32-2	REG_SZ	V2.0 Action=Block Dir=out App=C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe Svc=clr_optimization_v2.0.50727_32 Name=Block traffic for clr_optimization_v2.0.50727_32
DHCP-1	REG_SZ	V2.0 Action=Allow Dir=Out LPORT=68 RPORT=67 Protocol=17 App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102 Desc=@%SystemRoot%\system32\dhcpcsvc.dll,-102
DHCP-1-1	REG_SZ	V2.0 Action=Allow Dir=In LPORT=68 RPORT=67 Protocol=17 App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102 Desc=@%SystemRoot%\system32\dhcpcsvc.dll,-102
DHCP-2	REG_SZ	V2.0 Action=Allow Dir=In LPORT=546 RPORT=547 Protocol=17 App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102 Desc=@%SystemRoot%\system32\dhcpcsvc.dll,-102
DHCP-3	REG_SZ	V2.0 Action=Allow Dir=Out LPORT=546 RPORT=547 Protocol=17 App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102 Desc=@%SystemRoot%\system32\dhcpcsvc.dll,-102
DHCP-4	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102
DHCP-5	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=DHCP Name=@%SystemRoot%\system32\dhcpcsvc.dll,-102
dot3svc-1	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=dot3svc Name=Block any traffic to and from dot3svc
dot3svc-2	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=dot3svc Name=Block any traffic to and from dot3svc
DPS-1	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=DPS Name=Block any other traffic to and from DPS
DPS-2	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=DPS Name=Block any other traffic to and from DPS
EHSTART-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=ehstart Name=Block any inbound traffic to ehstart
EHSTART-2	REG_SZ	V2.0 Action=Block Dir=out App=%SystemRoot%\system32\svchost.exe Svc=ehstart Name=Block any outbound traffic from ehstart
EMDMgmt-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=EMDMgmt Name=Block any traffic to and from EMDMgmt Service
EMDMgmt-2	REG_SZ	V2.0 Action=Block Dir=out App=%SystemRoot%\system32\svchost.exe Svc=EMDMgmt Name=Block any traffic to and from EMDMgmt Service
Eventlog-1	REG_SZ	V2.0 Action=Allow Dir=In LPort=RPC Protocol=6 App=%SystemRoot%\system32\svchost.exe Svc=EventLog Name=Allow RPC/TCP traffic to EventLog
Eventlog-2	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=EventLog Name=Block any traffic to EventLog
Eventlog-3	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=EventLog Name=Block any traffic from EventLog
HideServ-1	REG_SZ	V2.0 Action=Block Dir=in App=%windir%\System32\svchost.exe Svc=HideServ Name=Block any traffic to HideServ
HideServ-2	REG_SZ	V2.0 Action=Block Dir=out App=%windir%\System32\svchost.exe Svc=HideServ Name=Block any traffic from HideServ
IPBusEnum-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=IPBusEnum Name=Block any inbound traffic to IPBusEnum
IPBusEnum-2	REG_SZ	V2.0 Action=Block Dir=out App=%SystemRoot%\system32\svchost.exe Svc=IPBusEnum Name=Block any outbound traffic from IPBusEnum
LMHosts-1	REG_SZ	V2.0 Action=Allow Dir=Out LPort=53 Protocol=6 App=%SystemRoot%\system32\svchost.exe Svc=lmhosts Name=@%SystemRoot%\system32\lmhsvc.dll,-103
LMHosts-2	REG_SZ	V2.0 Action=Allow Dir=Out LPort=53 Protocol=6 App=%SystemRoot%\system32\svchost.exe Svc=lmhosts Name=@%SystemRoot%\system32\lmhsvc.dll,-103
LMHosts-3	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=lmhosts Name=@%SystemRoot%\system32\lmhsvc.dll,-103
LMHosts-4	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=lmhosts Name=@%SystemRoot%\system32\lmhsvc.dll,-103
MPSSVC-1	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=Mpsvc Name=@FirewallAPI.dll,-23306
MPSSVC-2	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=Mpsvc Name=@FirewallAPI.dll,-23307
Netman-1	REG_SZ	V2.0 Dir=In Action=Block App=%SystemRoot%\system32\svchost.exe Svc=Netman Name=Block all inbound traffic to Netman
Netman-2	REG_SZ	V2.0 Dir=Out Action=Block App=%SystemRoot%\system32\svchost.exe Svc=Netman Name=Block all outbound traffic from Netman
P2P Grouping Allow In	REG_SZ	V2.0 Action=Allow Dir=In App=%SystemRoot%\system32\svchost.exe Svc=P2PSvc LPort=3587 Protocol=6 Name=Allow Grouping to receive from port 3587
P2P Grouping Allow Out	REG_SZ	V2.0 Action=Allow Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=P2PSvc LPort=3587 Protocol=6 Name=Allow Grouping to send to port 3587
P2P Grouping Block In	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=p2psvc Name=Block Grouping from all other ports
P2P Grouping Block Out	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=p2psvc Name=Block Grouping to all other ports
P2P Ident Block In	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=p2pimsvc Name=Block Idman from all other ports
P2P Ident Block Out	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=p2pimsvc Name=Block Idman to all other ports
PcaSvc-1	REG_SZ	V2.0 Action=Block Dir=in App=%SystemRoot%\system32\svchost.exe Svc=PcaSvc Name=@pcasvc.dll,-3 Desc=@pcasvc.dll,-5
PcaSvc-2	REG_SZ	V2.0 Action=Block Dir=out App=%SystemRoot%\system32\svchost.exe Svc=PcaSvc Name=@pcasvc.dll,-4 Desc=@pcasvc.dll,-6
PNRP Allow In	REG_SZ	V2.0 Action=Allow Dir=In App=%SystemRoot%\system32\svchost.exe Svc=PNRPSvc LPort=3540 Protocol=17 Name=Allow PNRP to send to port 3540
PNRP Allow Out	REG_SZ	V2.0 Action=Allow Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=PNRPSvc LPort=3540 Protocol=17 Name=Allow PNRP to send to port 3540
PNRP Block In	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=PNRPSvc Name=Block PNRP from all other ports
PNRP Block Out	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=PNRPSvc Name=Block PNRP to all other ports
PolicyAgent-1	REG_SZ	V2.0 Action=Allow Dir=Out LPort=389 Protocol=6 App=%SystemRoot%\system32\svchost.exe Svc=PolicyAgent Name=@FirewallAPI.dll,-23301
PolicyAgent-2	REG_SZ	V2.0 Action=Allow Dir=Out LPort=389 Protocol=17 App=%SystemRoot%\system32\svchost.exe Svc=PolicyAgent Name=@FirewallAPI.dll,-23302 Desc=@FirewallAPI.dll,-23303
PolicyAgent-3	REG_SZ	V2.0 Action=Allow Dir=In LPort=RPC Protocol=6 App=%SystemRoot%\system32\svchost.exe Svc=PolicyAgent Name=@FirewallAPI.dll,-5010 Desc=@FirewallAPI.dll,-5011
PolicyAgent-4	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=PolicyAgent Name=@FirewallAPI.dll,-23304
PolicyAgent-5	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=PolicyAgent Name=@FirewallAPI.dll,-23305
SearchFilterHost-1	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\SearchFilterHost.exe Name=Block all inbound traffic to SearchFilterHost
SearchFilterHost-2	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\SearchFilterHost.exe Name=Block all outbound traffic from SearchFilterHost
SearchIndexer-1	REG_SZ	V2.0 Action=Block Dir=In App=%SystemRoot%\system32\SearchIndexer.exe Svc=WSearch Name=Block all inbound traffic to SearchIndexer
SearchIndexer-2	REG_SZ	V2.0 Action=Block Dir=Out App=%SystemRoot%\system32\SearchIndexer.exe Svc=WSearch Name=Block all outbound traffic from SearchIndexer

More flexible exceptions

Active Directory user/computer accounts and groups

Source and destination IP addresses (individual or

range)

Source and destination TCP/UDP ports

Comma-delimited list of ports (but not low-high range)

IP protocol number

Types of interfaces (wired, wireless, VPN/RAS)

ICMP type and code

Services (used by service profiling to limit access)

Network profile

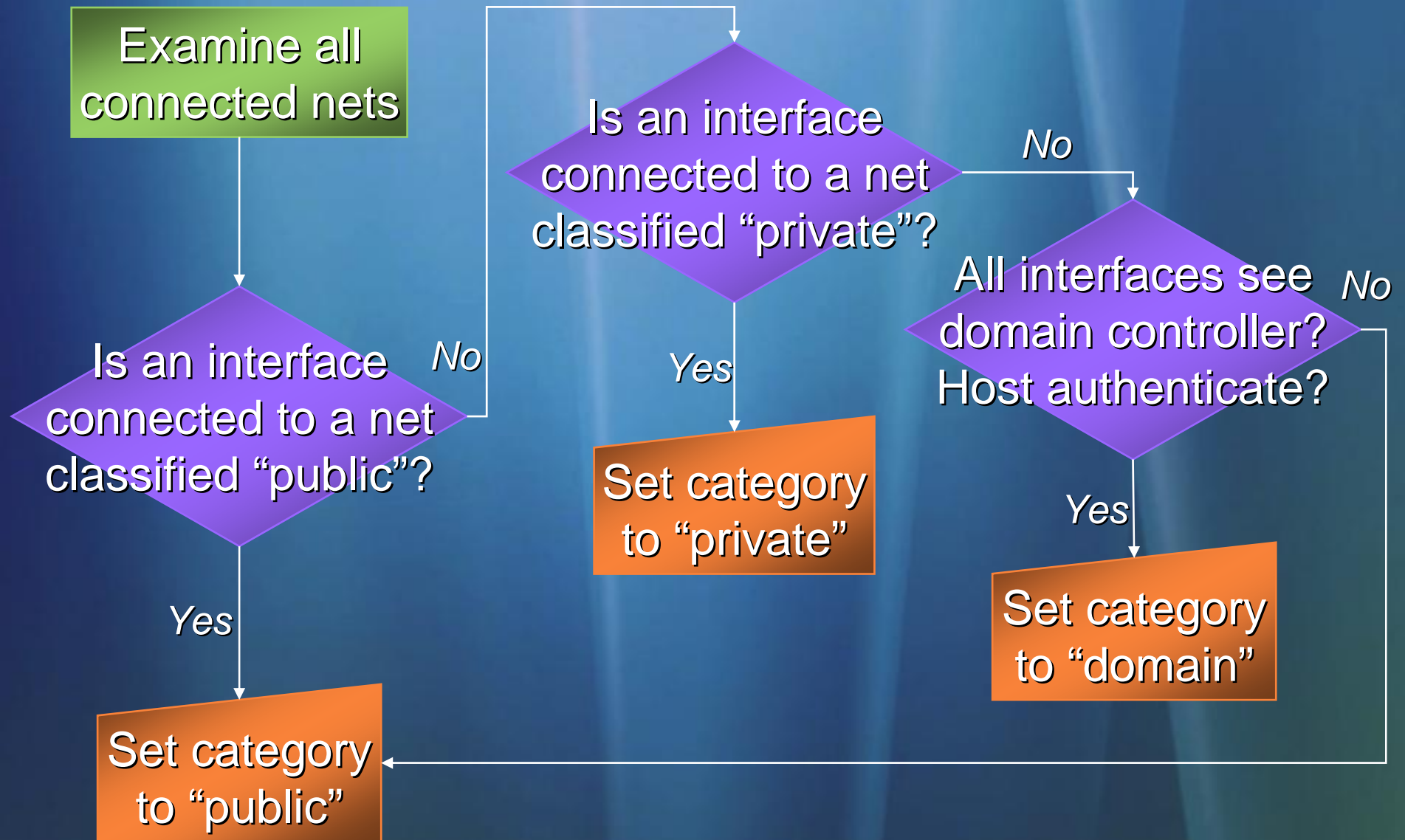
Domain When the computer is domain-joined and connected to the domain; automatically selected

Private When the computer is connected to a defined private network

Public All other networks

- NLA detects network changes
 - Identifies characteristics, assigns a GUID
- Network profile service creates profile upon connection
 - Interfaces, DC, authenticated machine, gateway MAC, ...
- NPS notifies firewall whenever NLA detects change
 - Firewall changes category within 200ms
- If not domain, user is queried for public or private
 - Must be local administrator to define a private network

What if multiple interfaces?

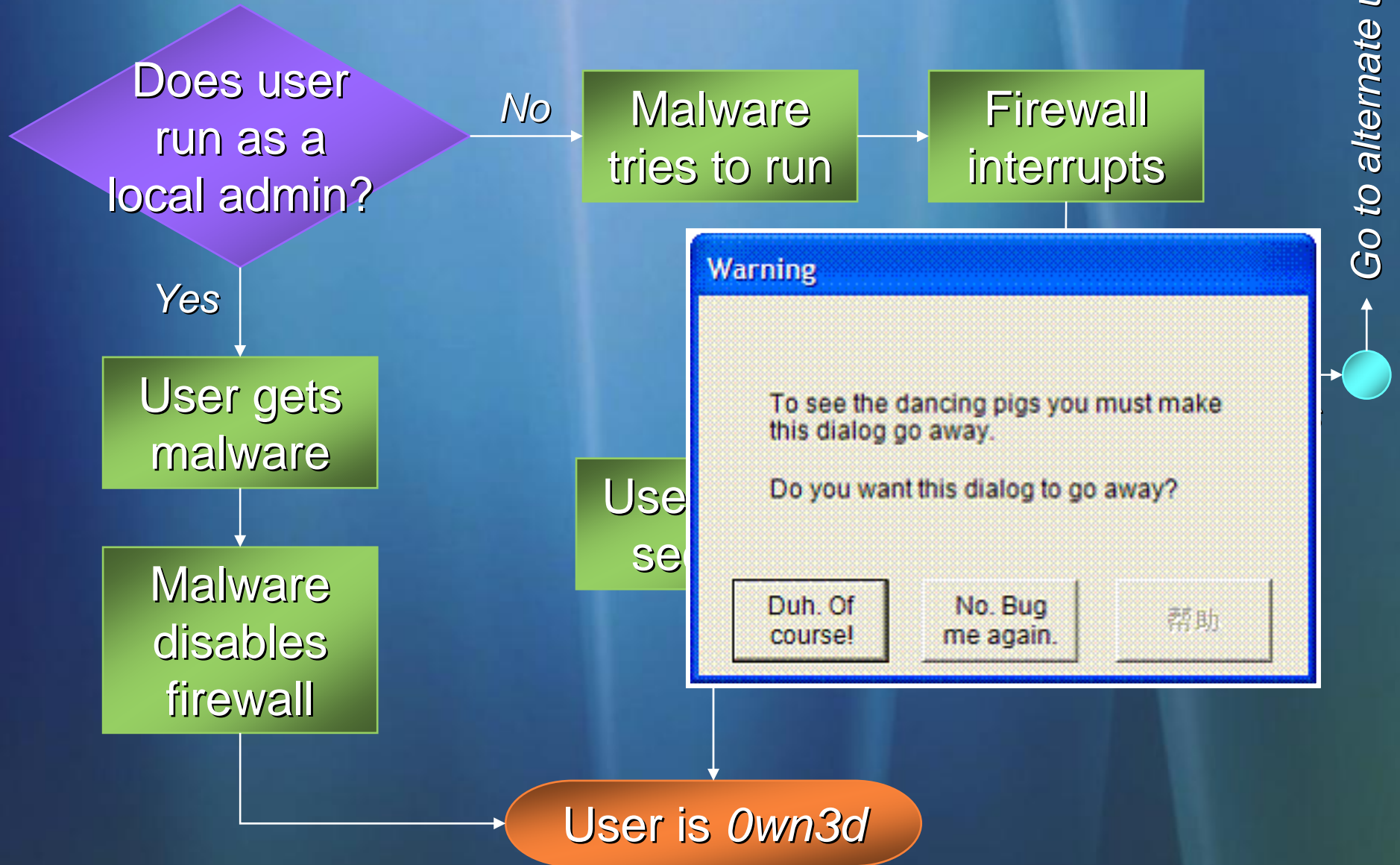


Group policy processing

- Previously, this is what you got—
 - Computer policies: when OS boots
 - User policies: when user logs on
 - Periodic refresh
- Now you also get—
 - Computer and user: upon establishing VPN connection
 - Computer and user: when computer resumes from hibernation or standby
- FW/IPsec policy is, of course, per-computer only

Did He Say Outbound Control?

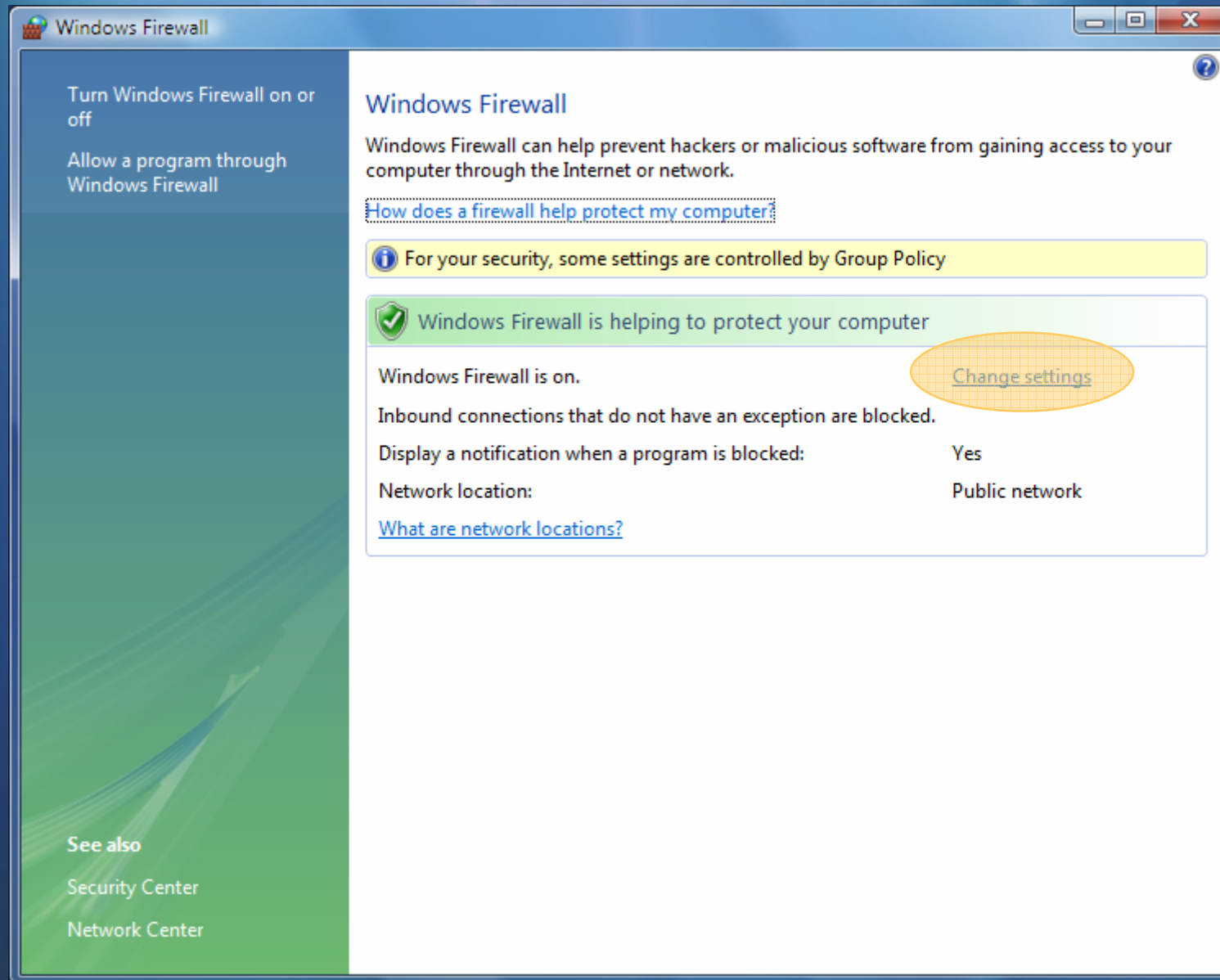
Why other host firewalls still suck

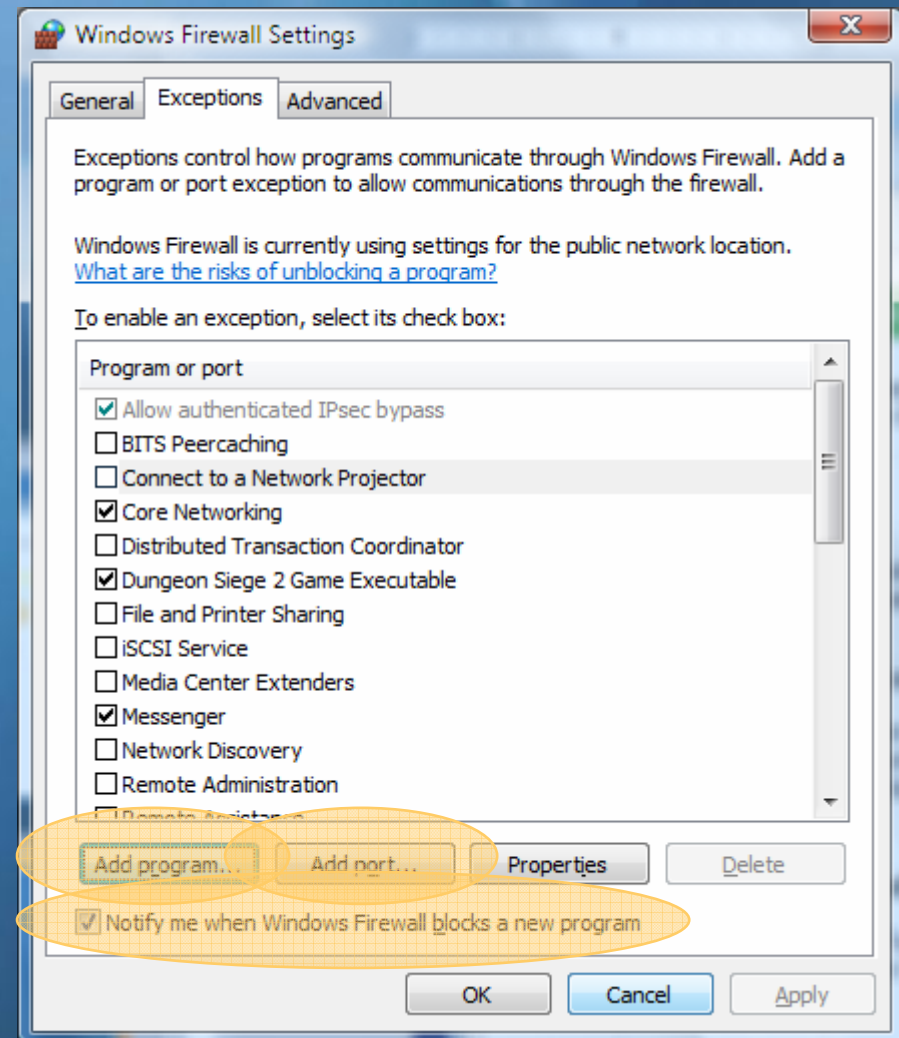
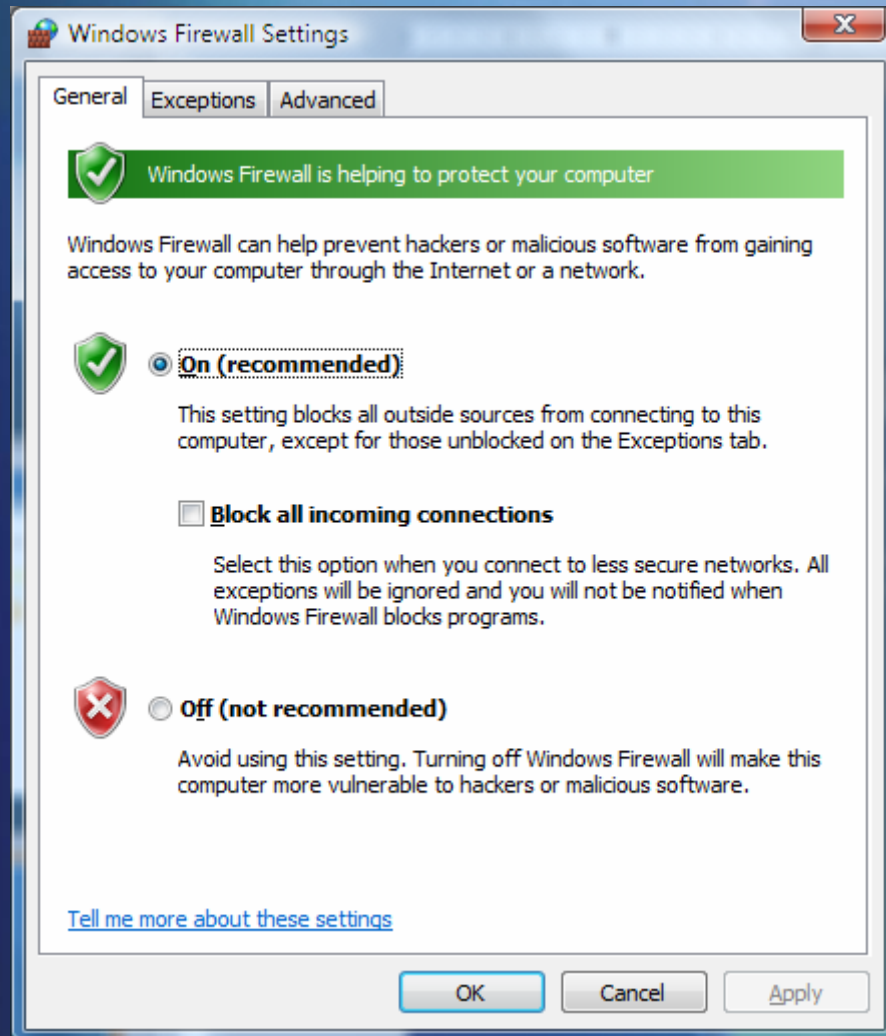


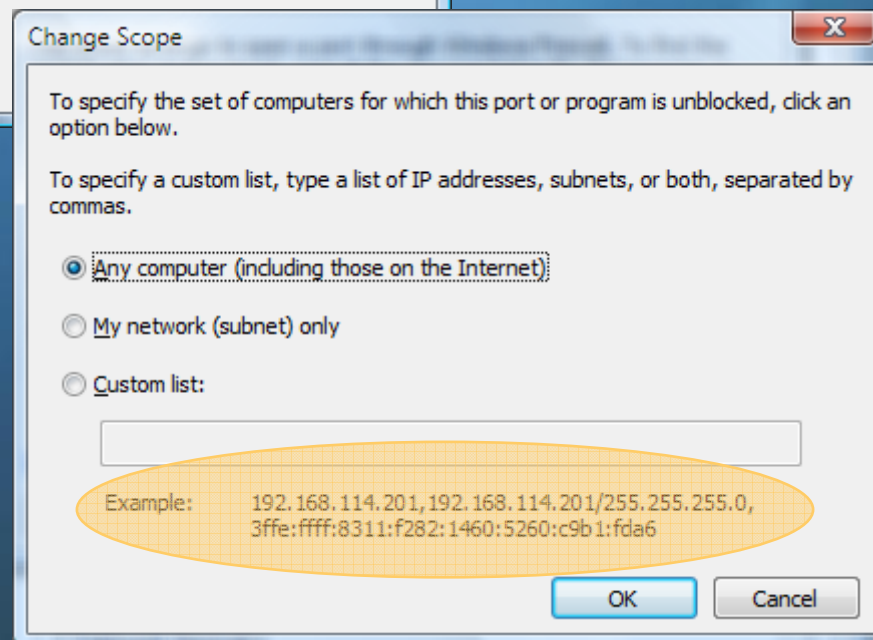
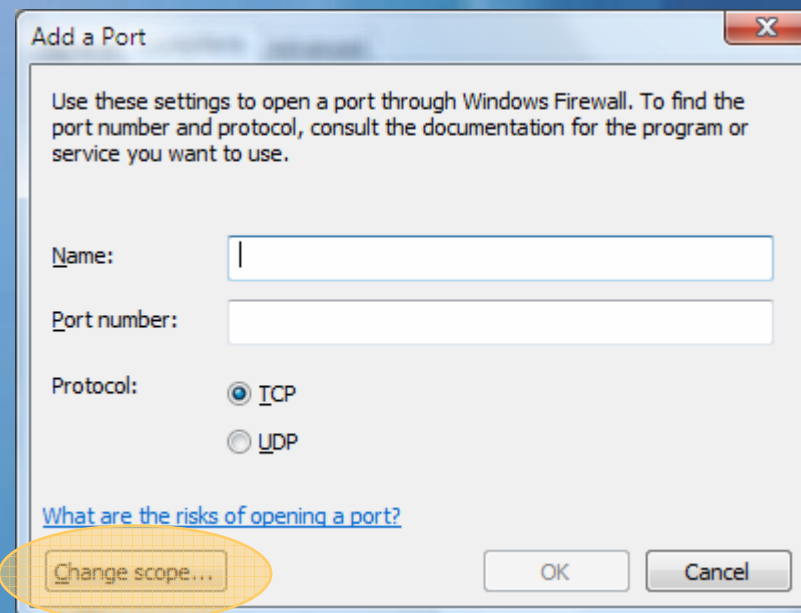
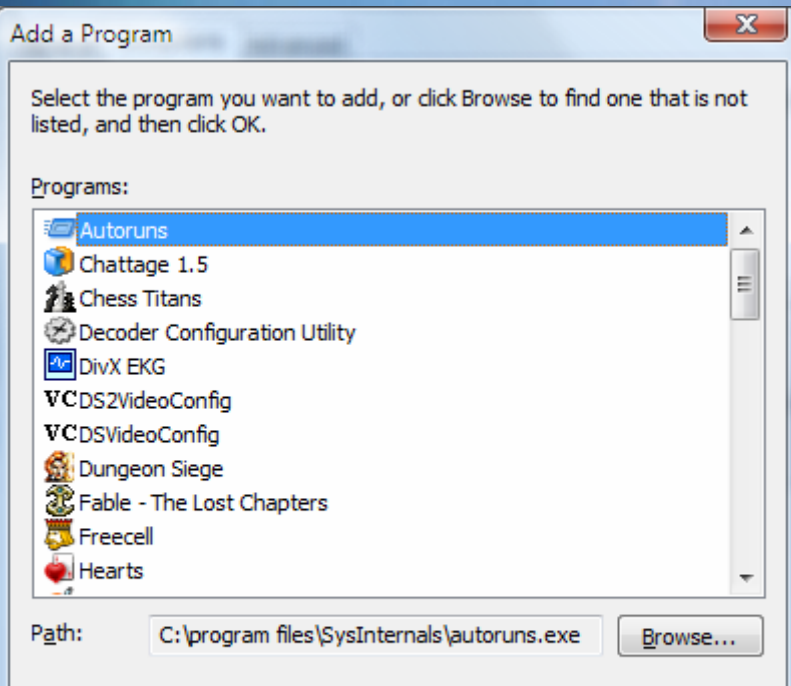
Therefore

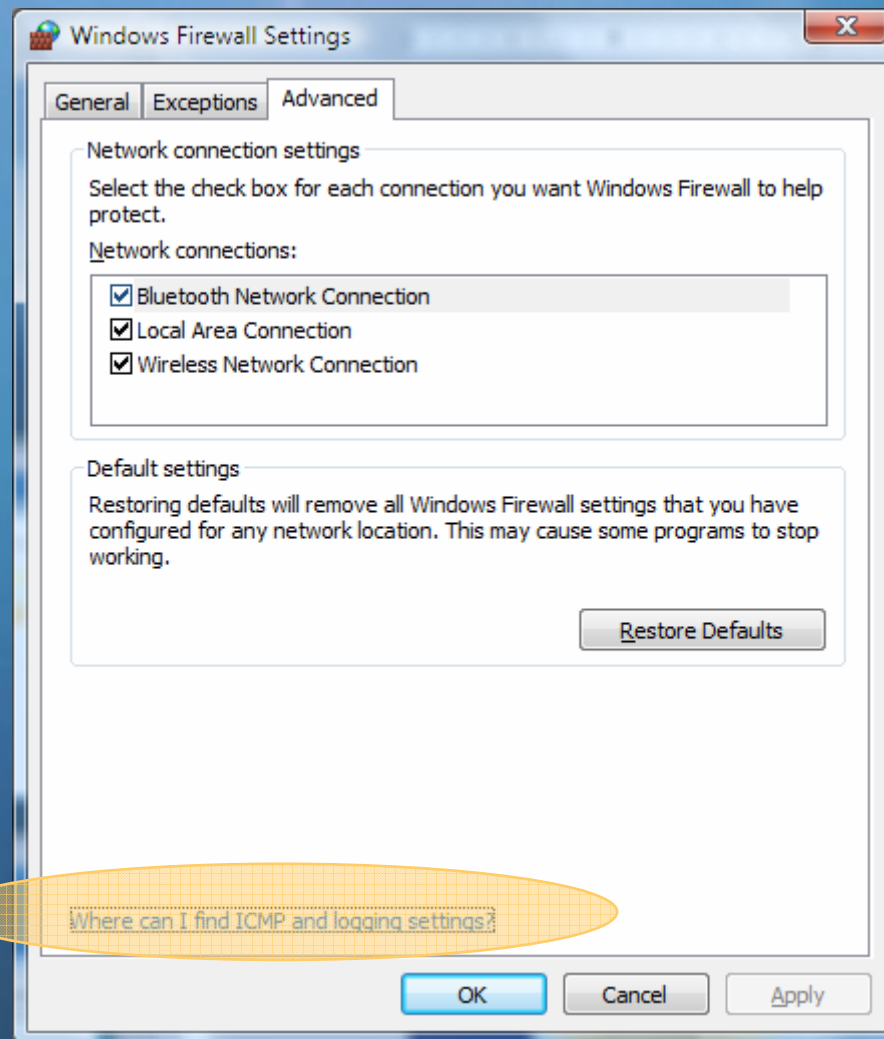
- Outbound control works only on machines that aren't compromised and operated by people who care about security
- Outbound control won't work where you want it to: on compromised machines or those operated by people who don't care about security
- Outbound control *is* useful for administratively restricting known software from communicating
- Switch off the prompting

Configuring The Firewall Control Panel

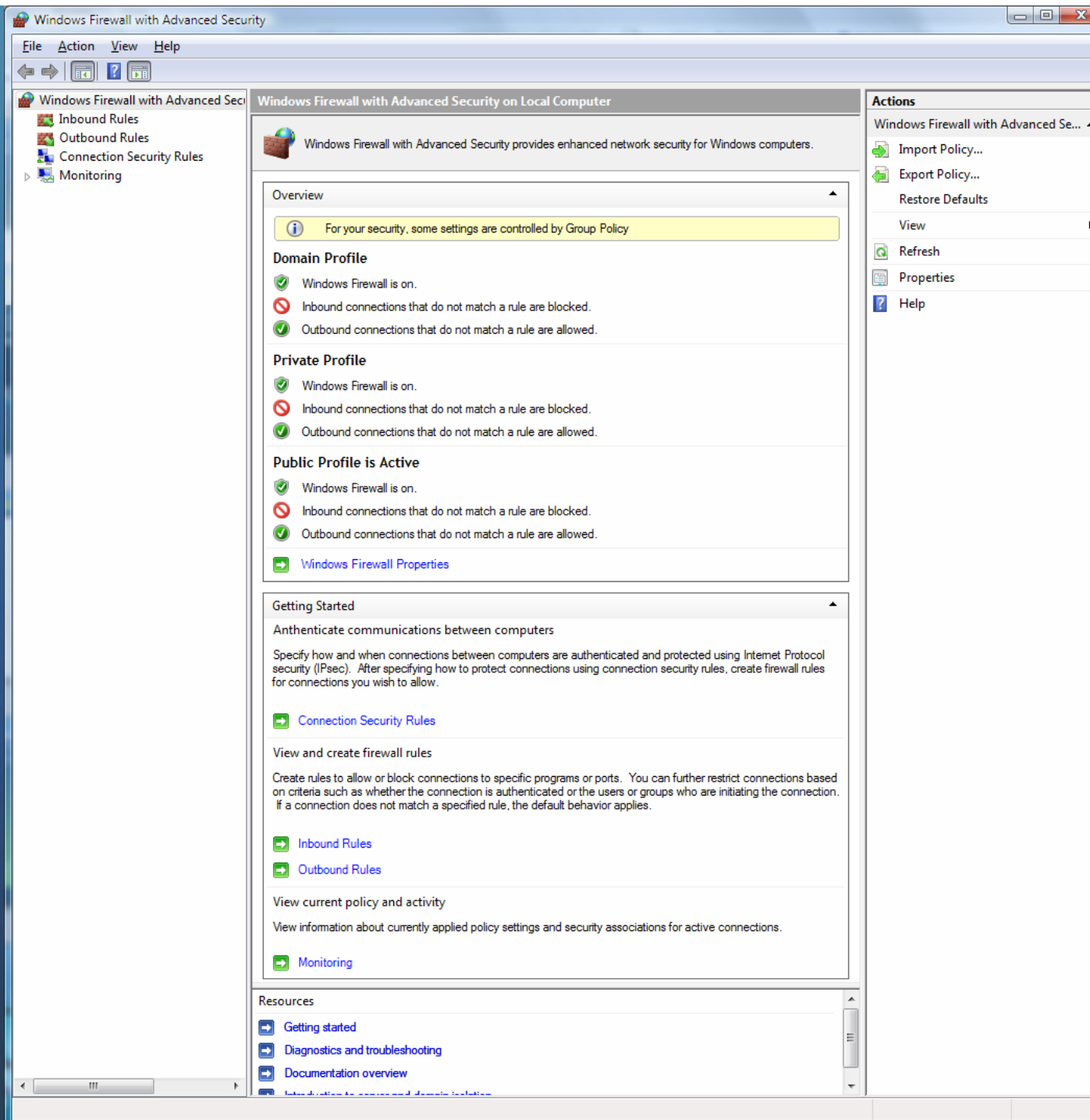




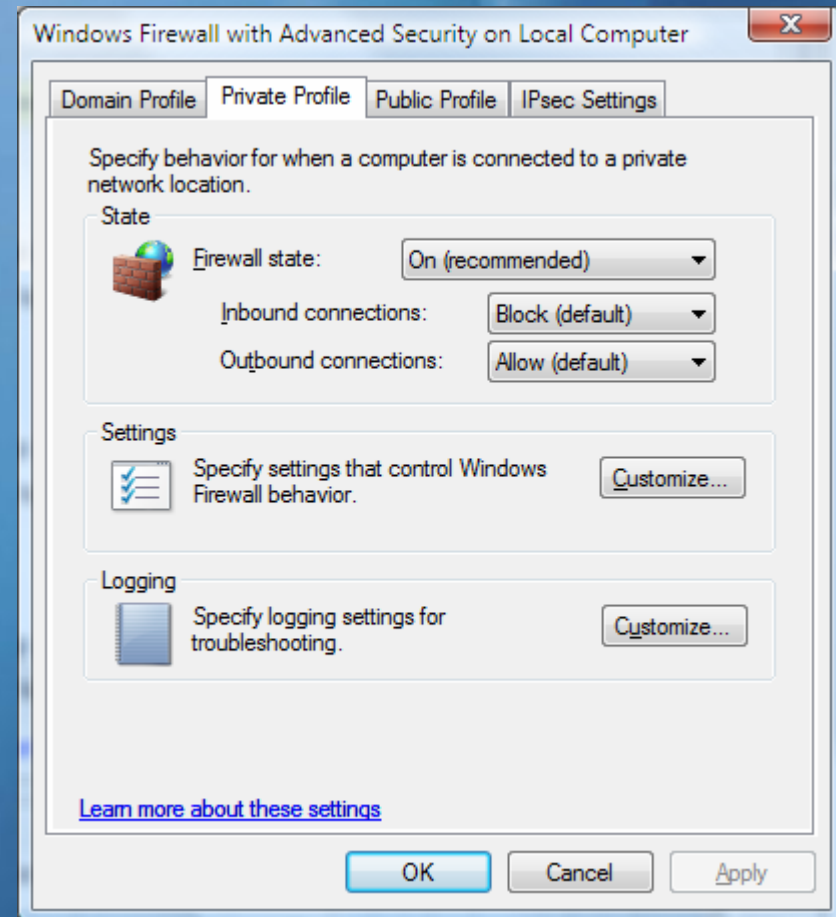
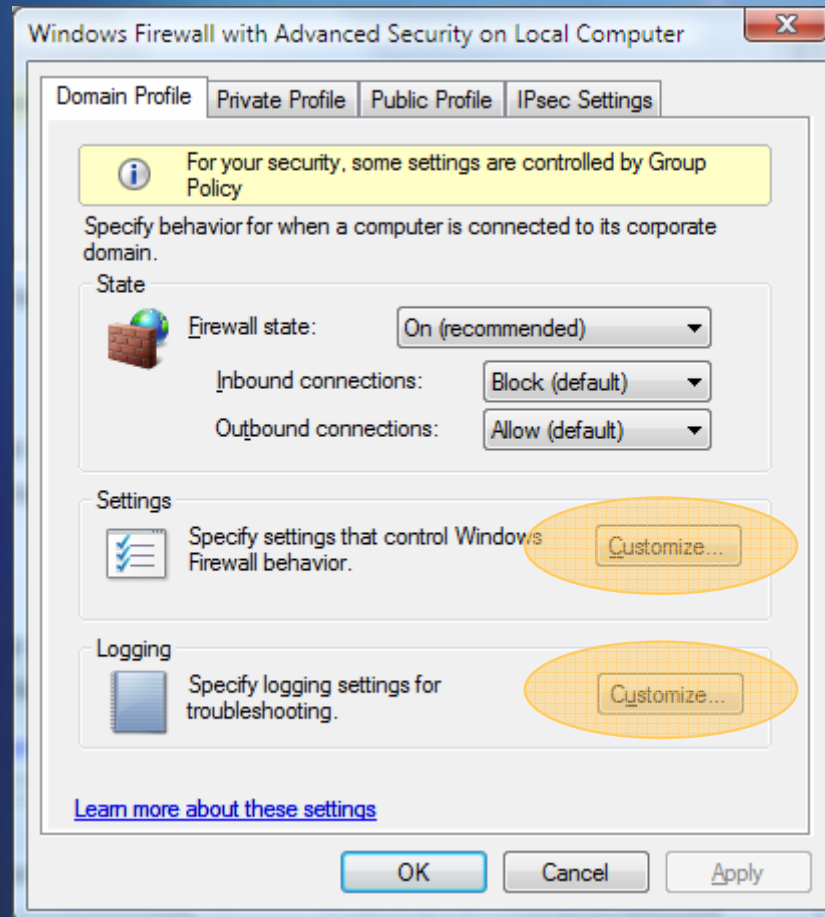




Configuring The Firewall Rules



Global settings



Global settings

Customize Settings for the Private Profile

Specify settings that control Windows Firewall with Advanced Security behavior.

Firewall settings
Display notifications to the user when a program is blocked from receiving inbound connections.

Display a notification: Yes (default)

Unicast response
Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: Yes (default)

Rule merging
Merging of rules created by local administrators with rules distributed through Group Policy. These setting can only be applied through Group Policy.

Apply local firewall rules: Yes (default)

Apply local connection security rules: Yes (default)

[Learn more about these settings](#)

OK Cancel

Customize Logging Settings for the Private Profile

Name: \system32\LogFiles\Firewall\pfirewall.log Browse...

Size limit (KB): 4,096

Log dropped packets: No (default)

Log successful connections: No (default)

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %windir%\system32\logfiles\firewall\pfirewall.log.

[Learn more about logging](#)

OK Cancel

Creating a rule

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advanced Security

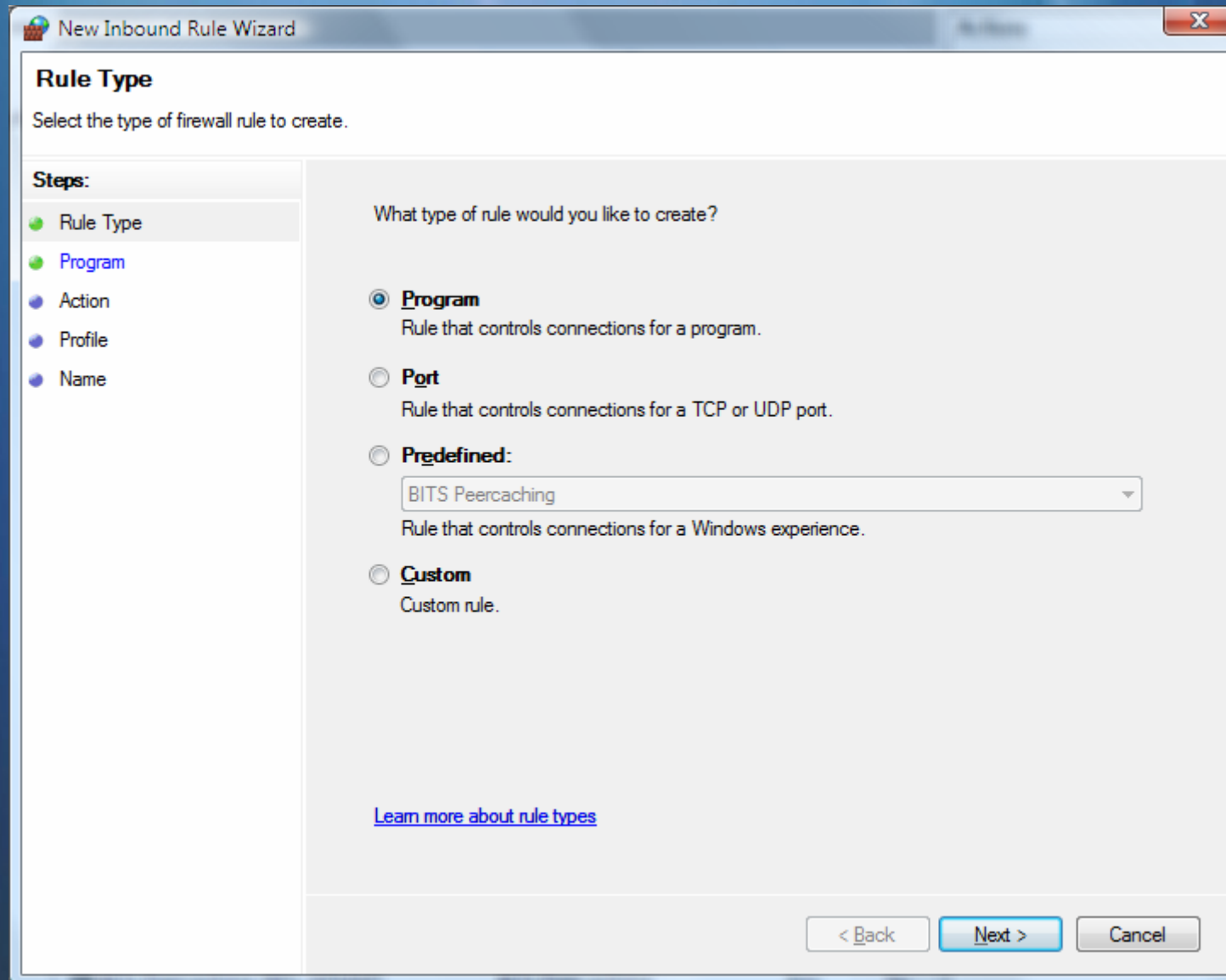
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed Users	Allowed Computers
Communicator		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Communicator		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Dungeon Siege 2 Game Executable		Public	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Dungeon Siege 2 Game Executable		Public	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
File Transfer Program		Domain	Yes	Allow	No	C:\windo...	Any	Any	TCP	Any	Any	Any	Any
File Transfer Program		Domain	Yes	Allow	No	C:\windo...	Any	Any	UDP	Any	Any	Any	Any
Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any	Any
Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any	Any
Microsoft Office Outlook		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	6004	Any	Any	Any
Rise of Nations		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Rise of Nations		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! FT Server		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! FT Server		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! Messenger		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! Messenger		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
BITS Peercaching (Content-In)	BITS Peercaching	Any	No	Allow	No	System	Any	Local subnet	TCP	2178	Any	Any	Any
BITS Peercaching (RPC)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	TCP	Dynamic...	Any	Any	Any
BITS Peercaching (RPC-EPMAP)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	TCP	RPC End...	Any	Any	Any
BITS Peercaching (WSD-In)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private, Public	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5357	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private, Public	No	Allow	No	System	Any	Local subnet	TCP	5357	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5358	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private, Public	No	Allow	No	System	Any	Local subnet	TCP	5358	Any	Any	Any
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	Any	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any
Core Networking - Destination Unreach...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Destination Unreach...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	Any	Yes	Allow	No	%System...	Any	Any	UDP	68	Any	Any	Any
Core Networking - Internet Group Mana...	Core Networking	Any	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	Any	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Do...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Qu...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Neighbor Discovery A...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Neighbor Discovery S...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Packet Too Big (ICMP...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Parameter Problem (I...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Router Advertisement...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Teredo (UDP-In)	Core Networking	Any	Yes	Allow	No	%System...	Any	Any	UDP	Edge Tra...	Any	Any	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Distributed Transaction Coordinator (TC...	Distributed Transaction Co...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Distributed Transaction Coordinator (TC...	Distributed Transaction Co...	Private, Public	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any	Any

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help
- Communicator
- Disable Rule
- Delete
- Properties
- Help

Rule types



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

☒ **Program**
Rule that controls connections for a program.

☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
BITS Peercaching
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

Rule types

The screenshot shows the 'New Inbound Rule Wizard' window. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type'. Below it, the instruction says 'Select the type of firewall rule to create.' On the left, a 'Steps:' pane lists five steps: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (blue dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main area asks 'What type of rule would you like to create?' and lists four options with radio buttons: 'Program' (Rule that controls connections for a program.), 'Port' (selected, Rule that controls connections for a TCP or UDP port.), 'Predefined:' (with a dropdown menu showing 'BITS Peercaching' and the description 'Rule that controls connections for a Windows experience.'), and 'Custom' (Custom rule.). At the bottom left is a link '[Learn more about rule types](#)'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted in blue), and 'Cancel'.

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

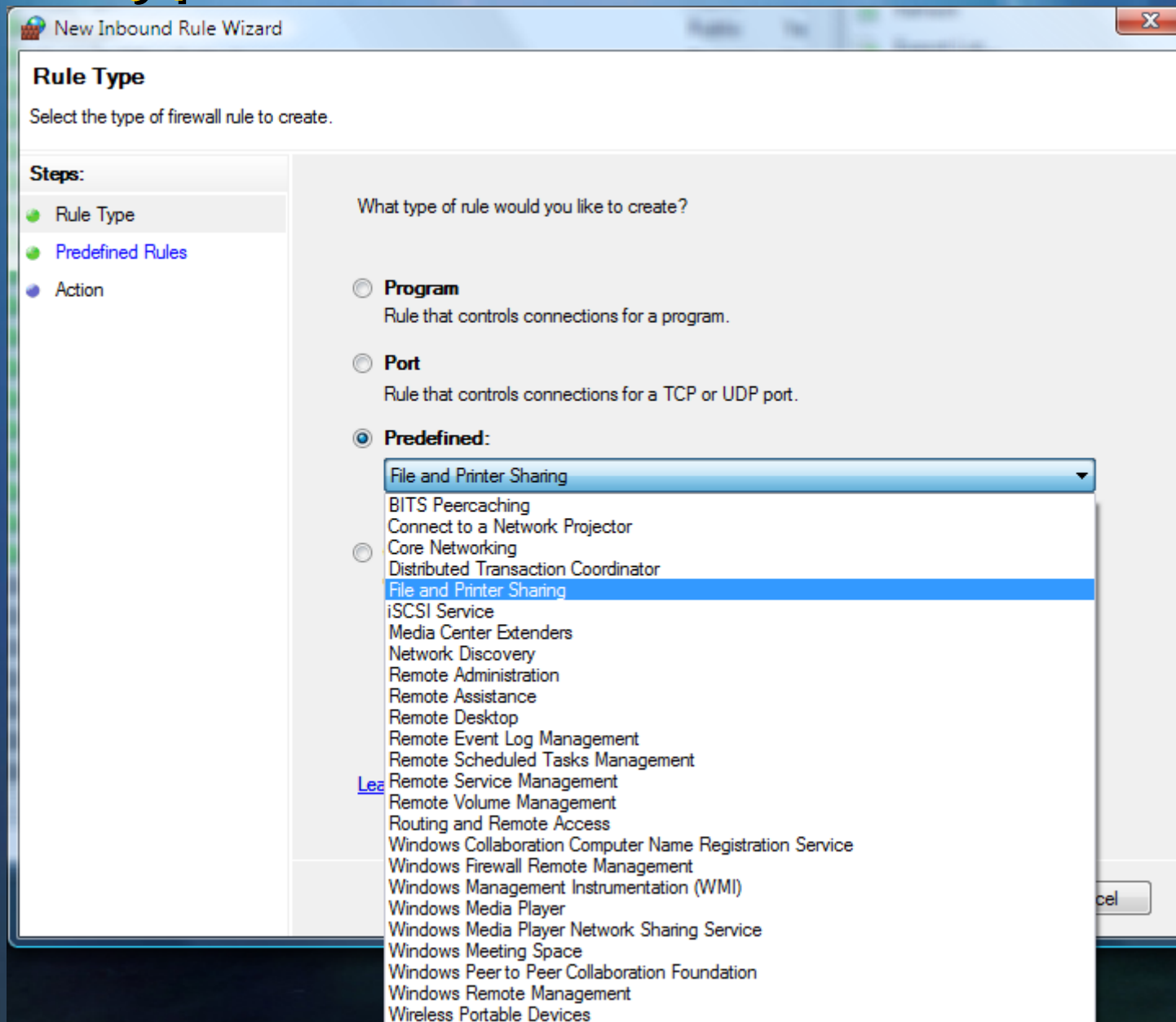
☐ **Predefined:**
BITS Peercaching
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

Rule types



Rule types

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**

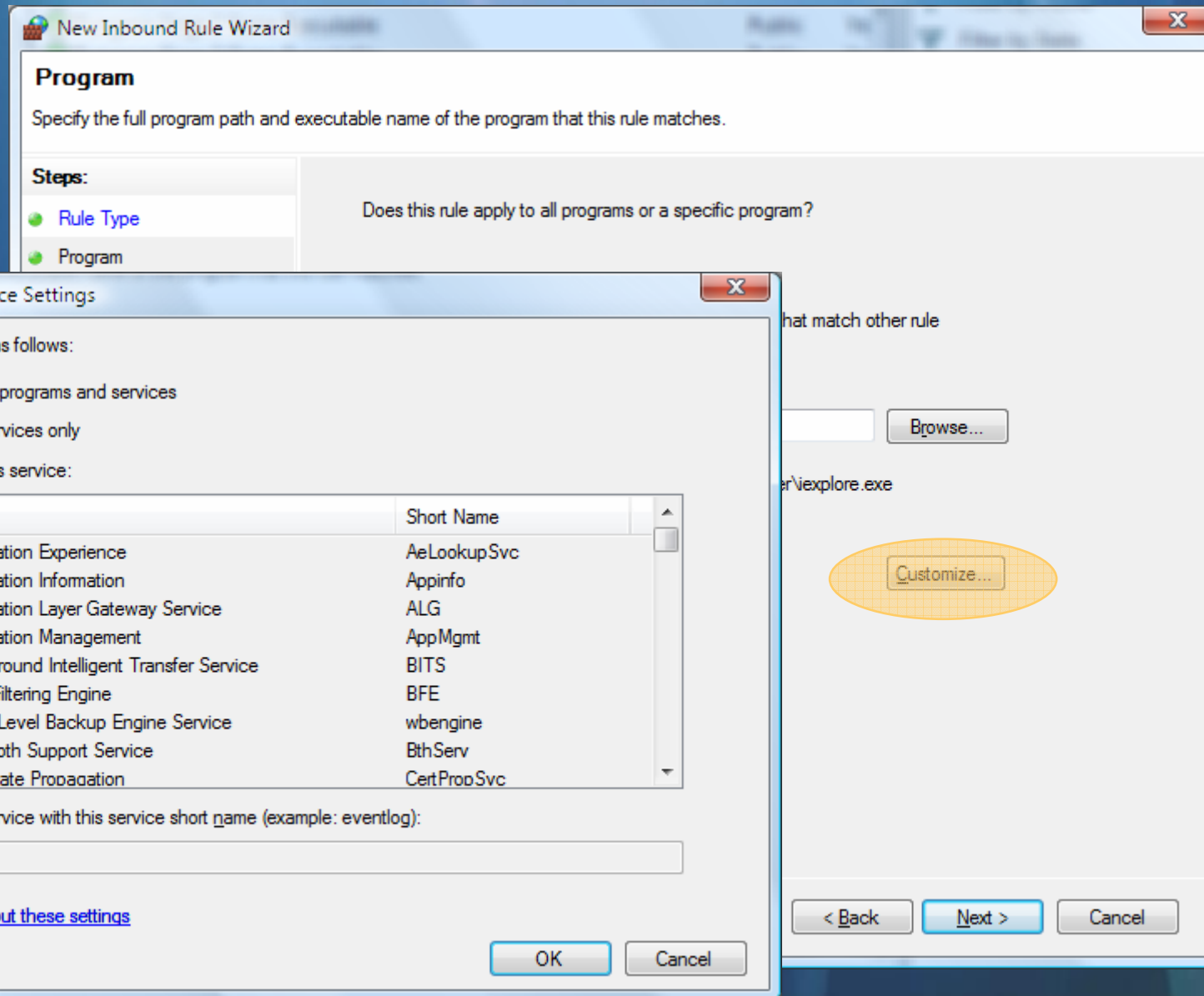
Rule that controls connections for a Windows experience.

☒ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

Program rule



Port rule

New Inbound Rule Wizard

Protocol and Ports

Specify the protocol and ports that this rule matches.

Steps:

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

What protocol and ports does this rule apply to?

Protocol type: Any

Protocol number: Any

Local port:

Remote port:

Internet Control Message (ICMP) settings:

[Learn more about protocol and ports](#)

< Back Next > Cancel

Port rule

New Inbound Rule Wizard

Protocol and Ports

Specify the protocol and ports that this rule matches.

Steps:

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

What protocol and ports does this rule apply to?

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Remote port: All Ports
Specific Ports
Dynamic RPC
RPC Endpoint Mapper
Edge Traversal

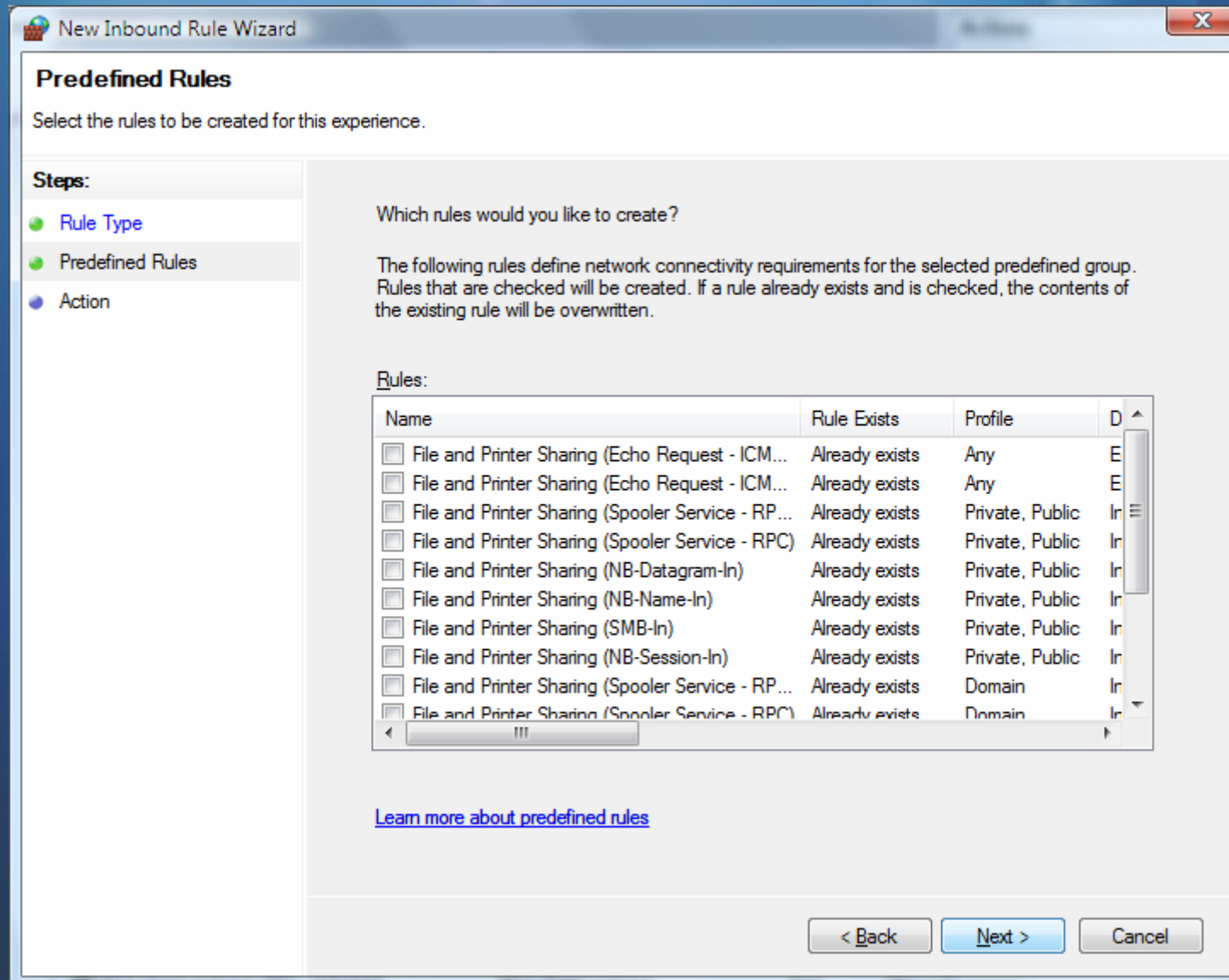
Example: 80, 445, 8080

Internet Control Message Protocol (ICMP) settings: Customize...

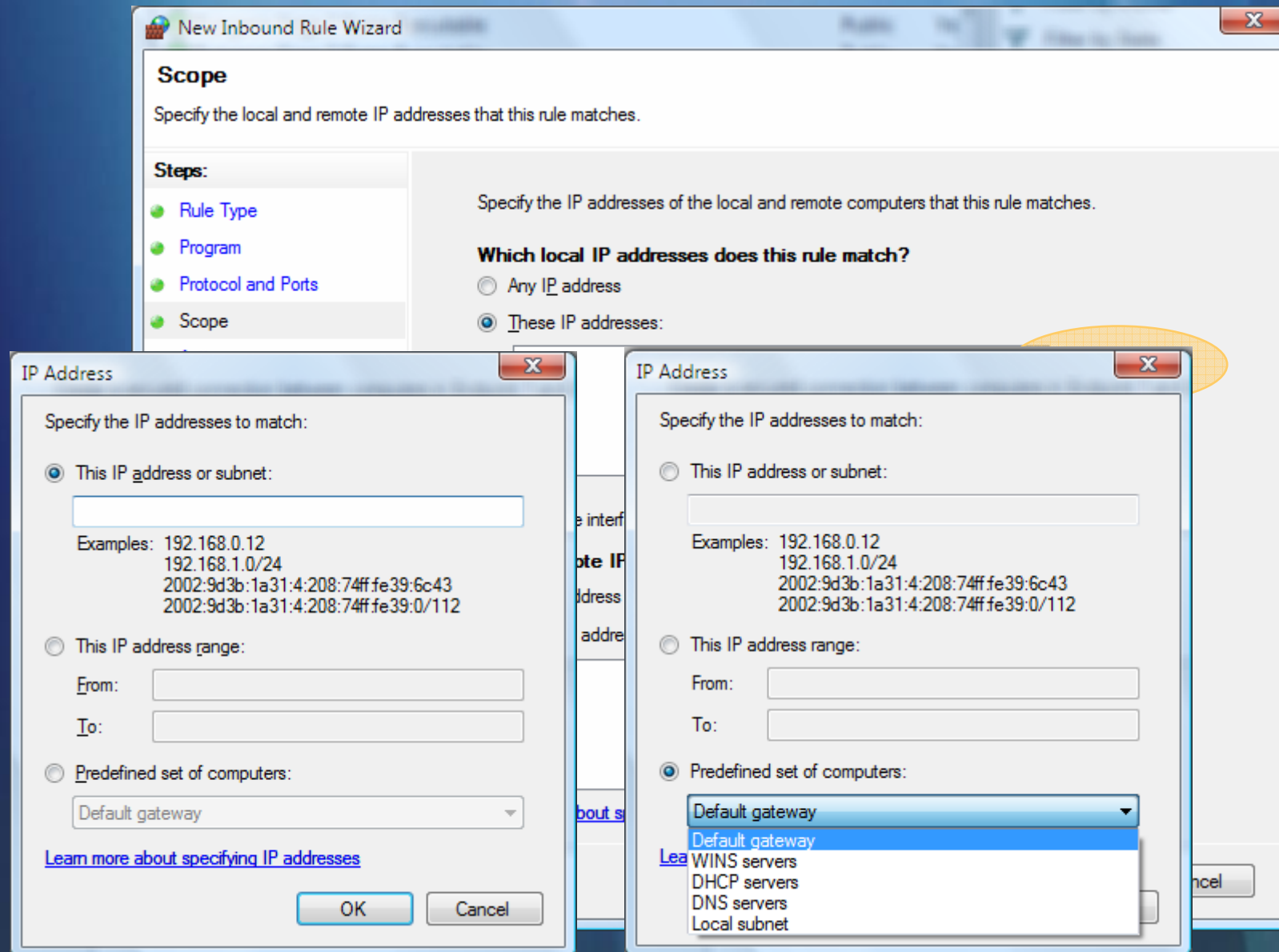
[Learn more about protocol and ports](#)

< Back Next > Cancel

Predefined rules



Scope



Scope

New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses that this rule matches.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

Specify the IP addresses of the local and remote computers that this rule matches.

Which local IP addresses does this rule match?

☐ Any IP address

☒ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule match?

☐ Any IP address

☐ These IP addresses:

[Learn more about specifying scope](#)

< Back Next > Cancel

Customize Interface Types

This rule applies to connections on the following interface types.

☒ All interface types

☐ These interface types:

☐ Local area network
☐ Remote access
☐ Wireless

[Learn more about interface types](#)

OK Cancel

Action

New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Profile
- Name

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

☒ **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

☐ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Require the connections to be encrypted**
Require privacy in addition to integrity and authentication.

☐ **Override block rules**
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

Action—secured with IPsec

The screenshot shows the 'New Inbound Rule Wizard' window. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action'. Below it, a subtitle says 'Specify the action that is taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action' (highlighted with a yellow oval), 'Users and Computers', 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?'. It offers three radio button options: 'Allow the connection' (with a description), 'Allow the connection if it is secure' (selected, with a description), and 'Block the connection' (with a description). Below these are two unchecked checkboxes: 'Require the connections to be encrypted' and 'Override block rules' (with a description). A link 'Learn more about actions' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Users and Computers
- Profile
- Name

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

☐ **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

☒ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Require the connections to be encrypted**
Require privacy in addition to integrity and authentication.

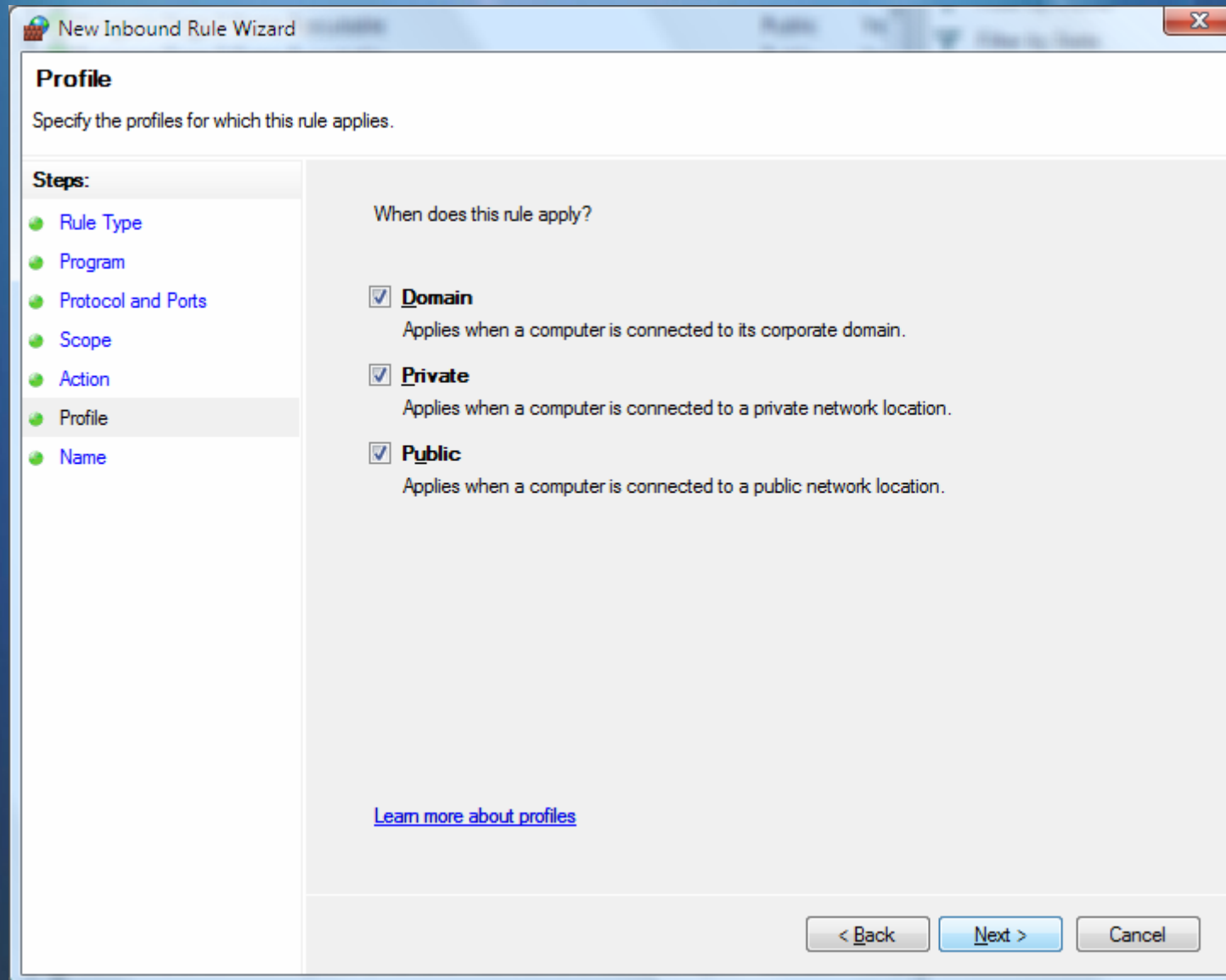
☐ **Override block rules**
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

Profile



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. The main content area is titled 'Profile' and contains the instruction 'Specify the profiles for which this rule applies.' On the left side, there is a 'Steps:' list with the following items: 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile' (which is highlighted), and 'Name'. Each item has a green circular icon to its left. The main area on the right is titled 'When does this rule apply?' and contains three checked options: 'Domain' (with a description 'Applies when a computer is connected to its corporate domain.'), 'Private' (with a description 'Applies when a computer is connected to a private network location.'), and 'Public' (with a description 'Applies when a computer is connected to a public network location.'). At the bottom of the main area, there is a link that says 'Learn more about profiles'. At the bottom right of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile**
- Name

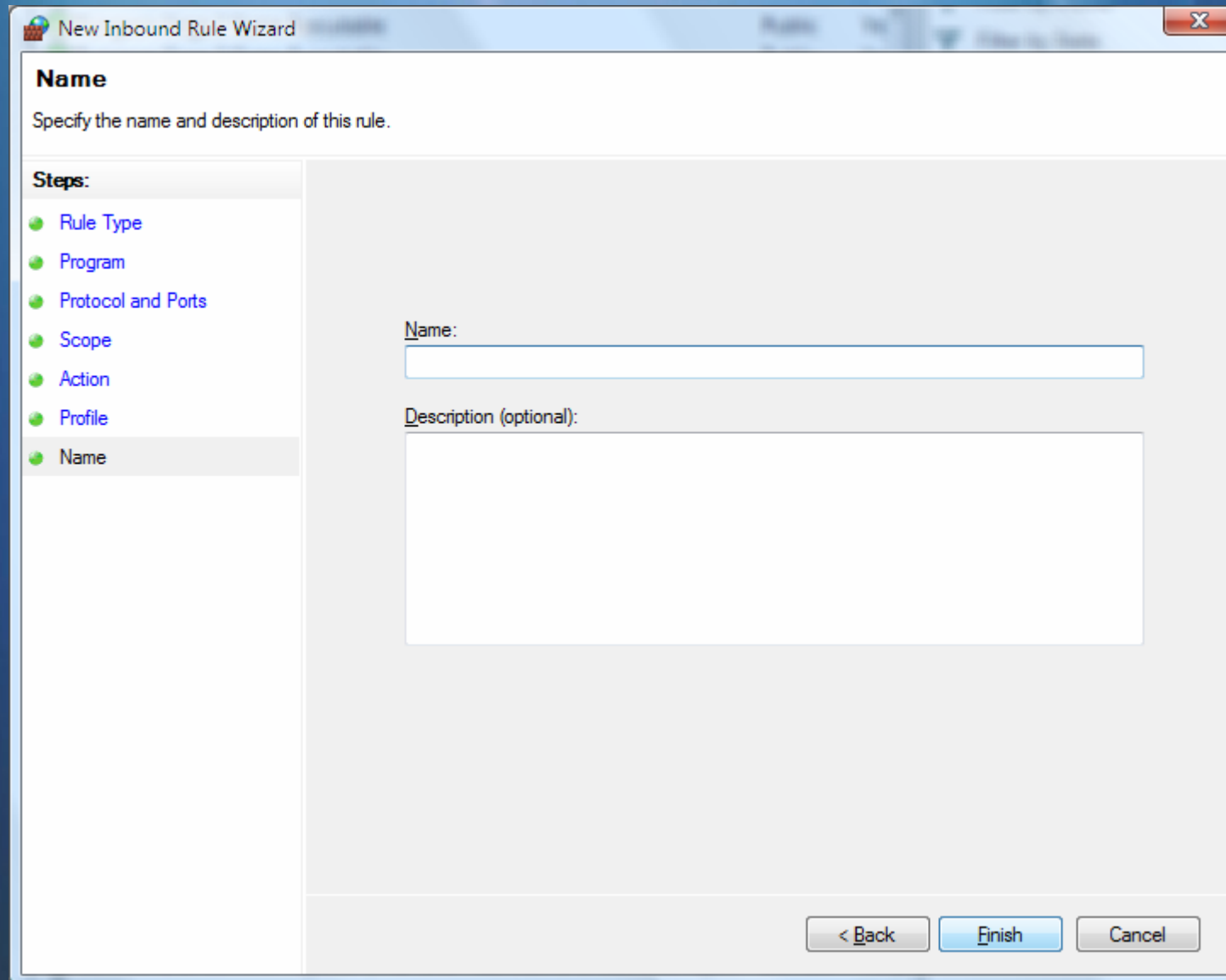
When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location.
- ☒ **Public**
Applies when a computer is connected to a public network location.

[Learn more about profiles](#)

< Back Next > Cancel

Name



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:

Description (optional):

< Back Finish Cancel

Controlling The Firewall

Programmatic interfaces

- INetFwPolicy2
 - Provides access to the policy
- INetFwRule
 - Provides access to rule properties
- INetFwRules
 - Provides access to a collection of firewall or Windows Service Hardening rules
- INetFwServiceRestriction
 - Provides access to the Windows Service Policy
- All defined in Netfw.h, requires FirewallAPI.dll

Is the firewall enabled?

```
option explicit
Dim CurrentProfile
' Create the FwPolicy2 object.
Dim fwPolicy2
Set fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
CurrentProfile = fwPolicy2.CurrentProfileTypes
if fwPolicy2.FirewallEnabled(CurrentProfile) <> TRUE then
    WScript.Echo("Firewall is disabled.")
else
    WScript.Echo("Firewall is enabled.")
end if
```

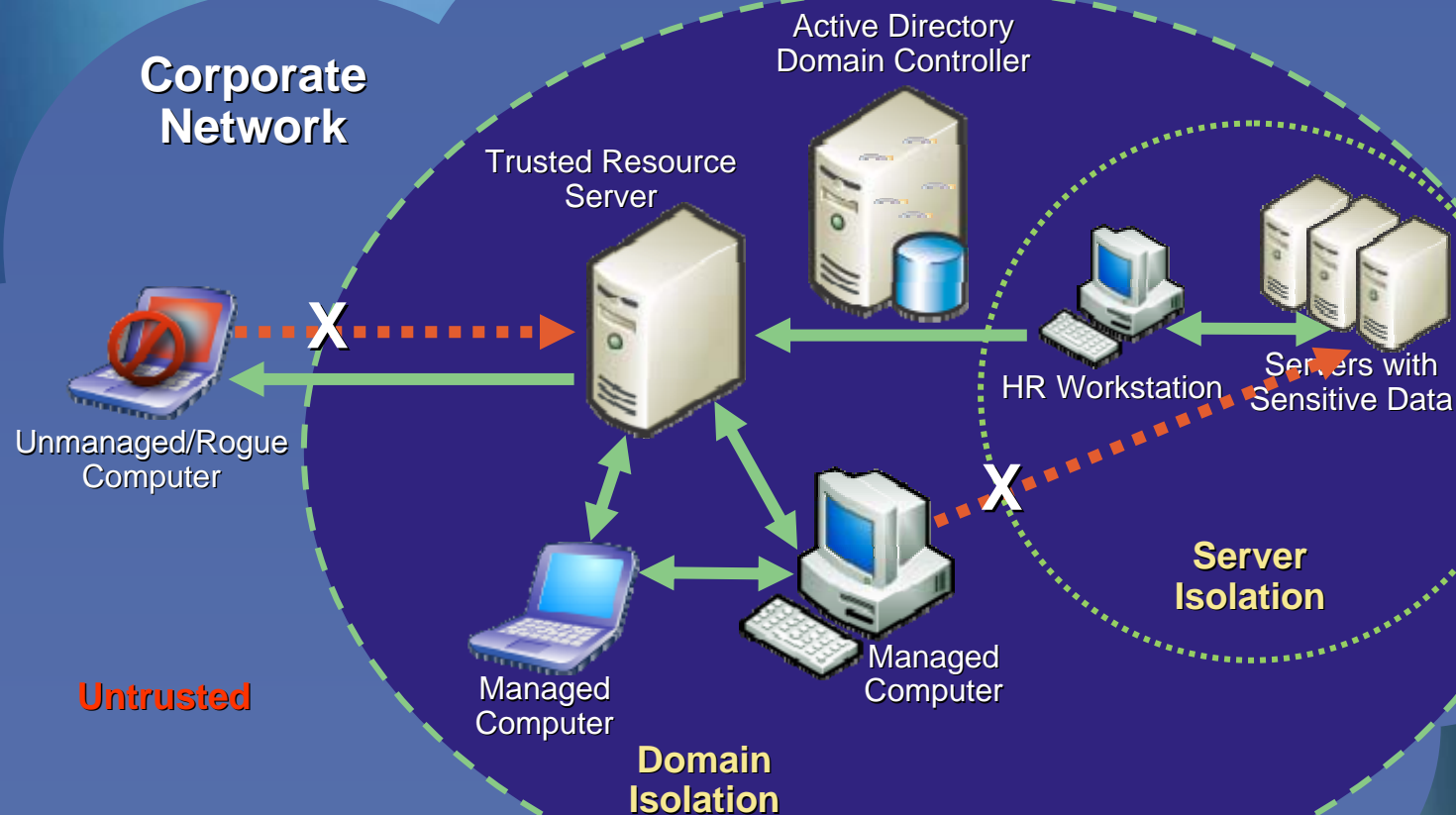

netsh advfirewall

- Full configuration interface
- Scriptable
 - Dump rules
 - Export rules
 - Import rules
 - Create rules
- Contexts for firewall rules and IPsec (connection security) rules
- Set and show global and per-profile properties
- Display active state (firewall rules, IPsec rules and security associations)



IPsec

Policy-based dynamic segmentation



Enable tiered-access to sensitive resources

Tame the beast

- Simplified policy configuration
- Client-to-DC protection
- Improved support for load balancing and clustering
- Improved authentication
- More cryptographic suites
- New configuration options
- More events and counters

Integrated with the firewall

- Eliminates confusion and rule overlap
- All firewall rules can be IPsec aware

“Allow application *foo* to receive traffic on port *bar* only if it’s authenticated (and optionally encrypted) by IPsec”

“Allow service *foo* to receive traffic from a remote computer or a remote user only if it’s identified by IKE”

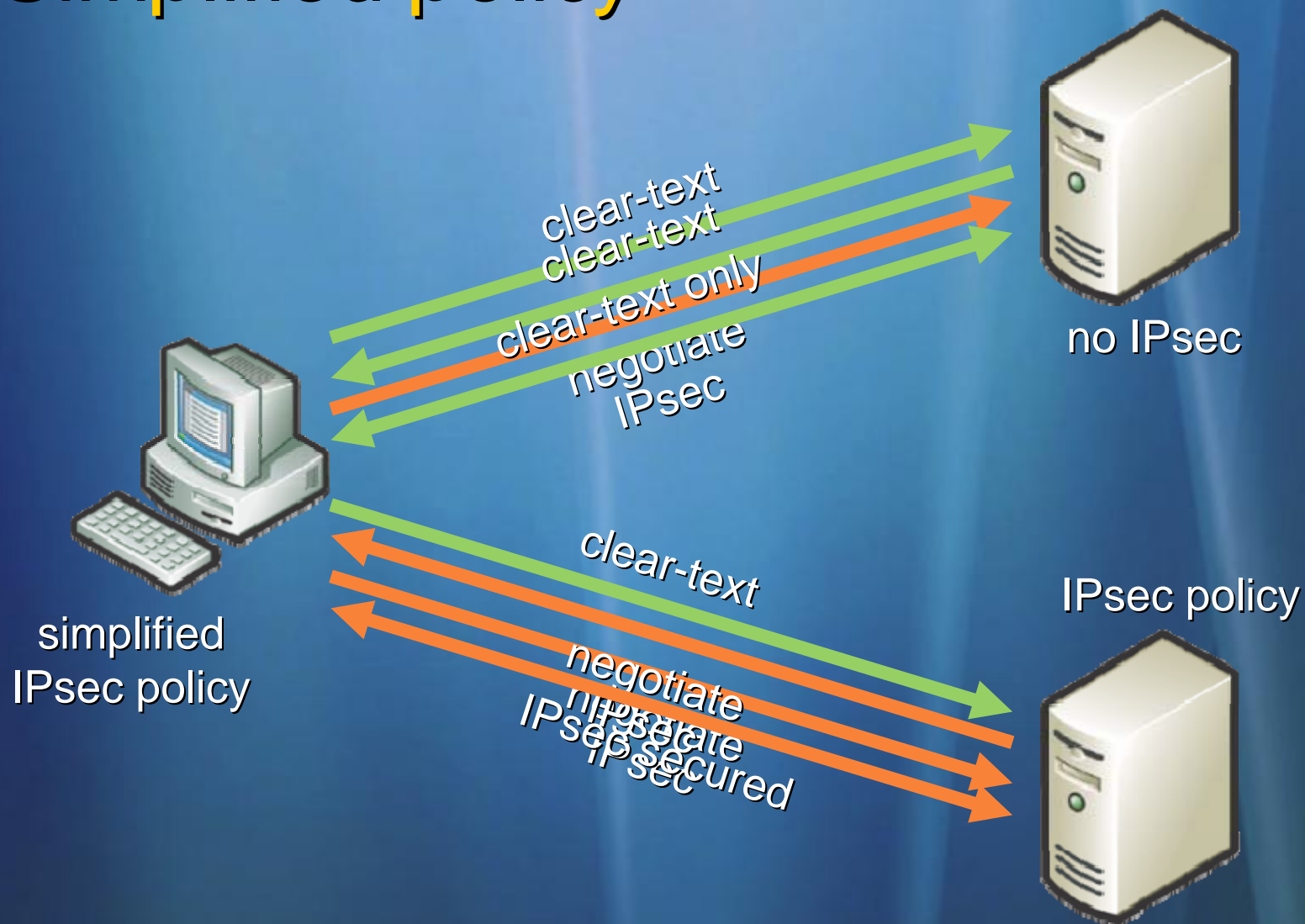
Isolation: authentication

- Here's your wizard for server and domain isolation
 - Request authN for inbound and outbound
 - Require authN for inbound, request for outbound
 - Require authN for inbound and outbound
- Authentication types—
 - Computer and user (with Kerberos)
 - Computer (with Kerberos)
 - Computer certificate
 - Health certificate (NAP)
 - Combinations

Simplified policy

- Initiator communicates to responder simultaneously in clear-text and with IPsec
 - Switch to IPsec if responder can support
 - Remain clear-text if not
- Eliminates delay issues with current “fall back to clear” implementation
- Eliminates need to create policies filled with exceptions for non-IPsec devices

Simplified policy



Working with domain controllers

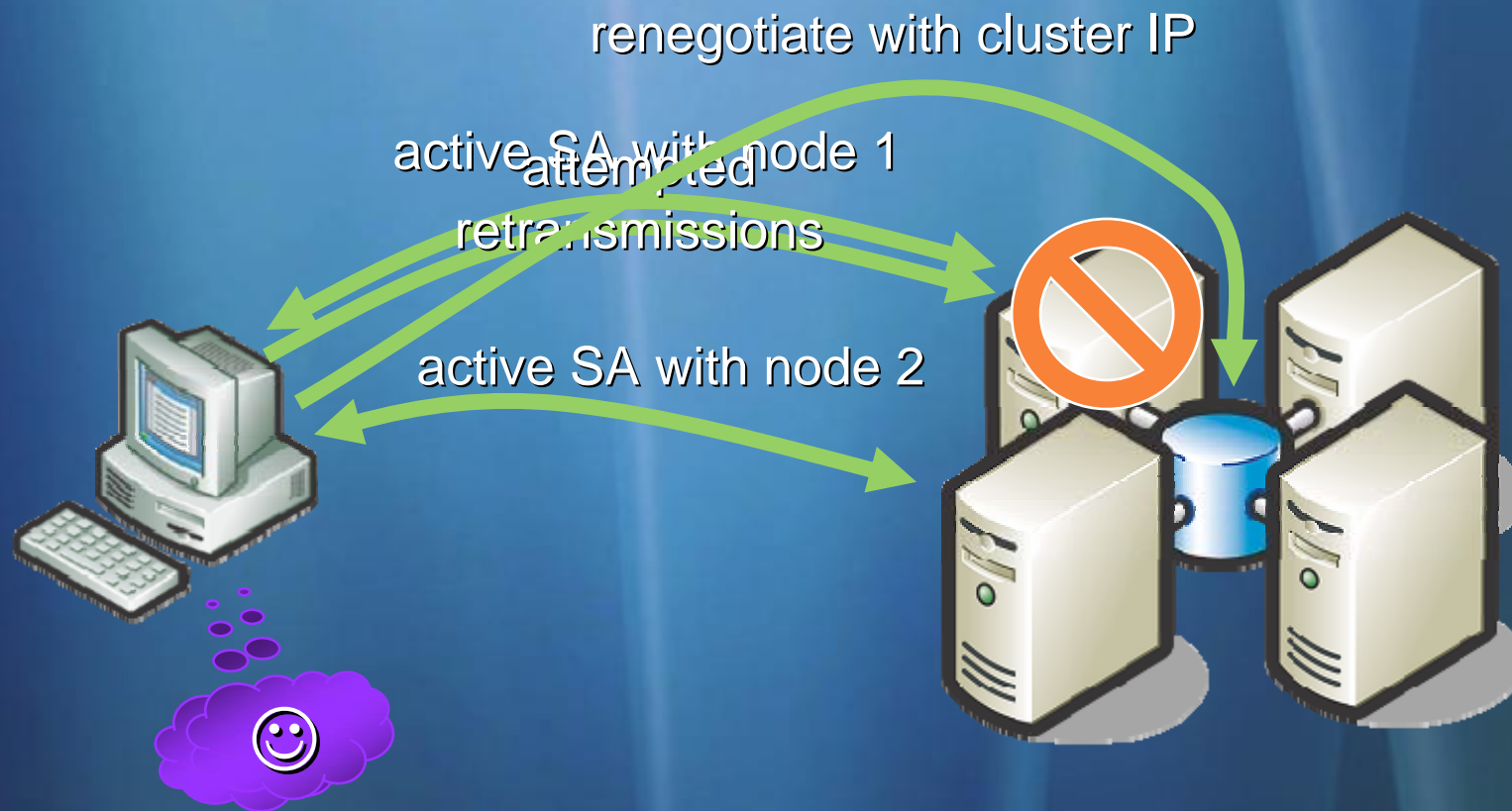
Configuring IPsec on ...will result in this

- | | |
|---------|---|
| Request | <ul style="list-style-type: none">• Domain joins and logons in clear text• Subsequent communications protected |
| Require | <ul style="list-style-type: none">• Domain joins will require entering user ID and password of a domain account• Works only on Windows Vista clients |

Load balancing and clustering

- 2000/XP/2003 take up to two minutes to re-establish connection when a node fails
 - 1 minute: idle time expiration
 - 1 minute: renegotiate security associations (SAs)
- Vista/Longhorn monitor established active SAs
 - If TCP connection begins retransmitting segments, this indicates that the peer is down
 - IPsec renegotiates SAs immediately with another node
 - Failover typically now won't affect app stability

Load balancing and failover



New cryptographic algorithms

Encryption

- AES-128
- AES-192
- AES-256

Key
exchange

- P-256 (DH group 19 elliptic curve)
- P-384 (DH group 20 elliptic curve)

Improved authentication

- Require a health certificate
- New “extended mode”
 - IKE extension known as AuthIP
 - User authentication: Kerberos, NTLMv2, certificate
 - Health certificates use extended mode
- Multiple methods tried
 - Doesn't give up after first fails
 - Tried in the specified order
 - Allows for differing authentication and crypto sets on individual SAs between a pair of peers
 - Although, why would you ever do this???

Rule actions



More flexible exceptions

Active Directory user/computer accounts and groups

Source and destination IP addresses (individual or

range)

Source and destination TCP/UDP ports

Comma-delimited list of ports (but not low-high range)

IP protocol number

Types of interfaces (wired, wireless, VPN)

ICMP type and code

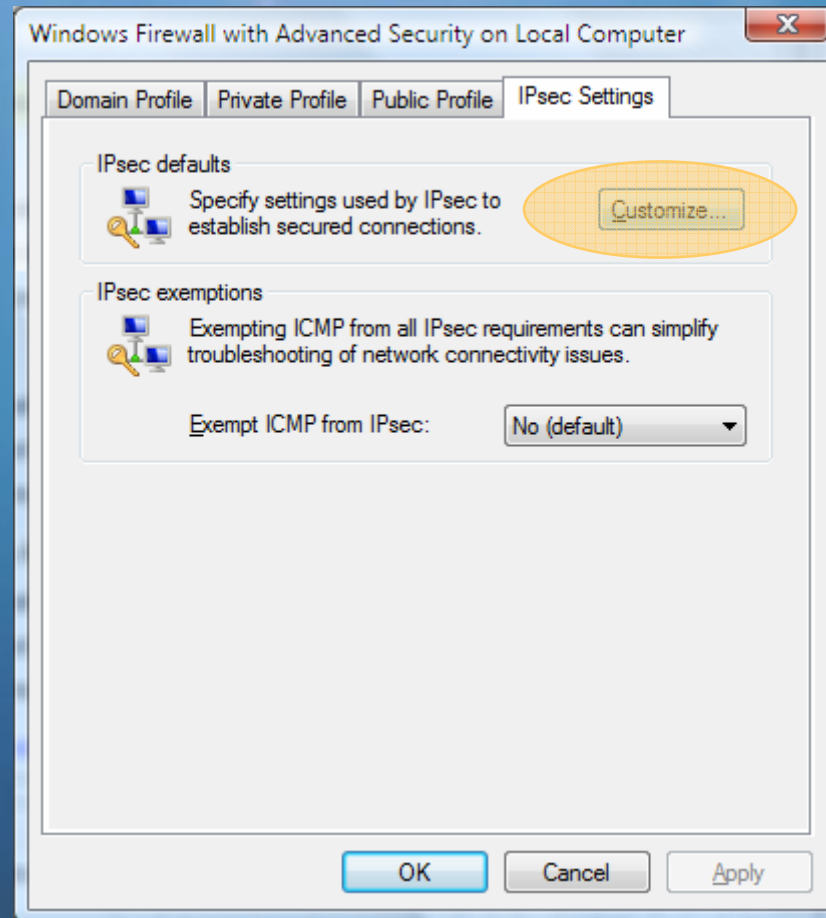
Services (used by service profiling to limit access)

- Most require IPsec-aware firewall rules to configure (can't be configured through connection security rules)

More about rules

- Ordering: same as current Windows
 - Ordered by specificity
 - ❶ AuthN bypass ❷ Block ❸ Allow
- Authenticated rules: firewall rules that are aware of IPsec protection
 - Make filtering decisions based on SAs
 - Do *not* control creating SAs: you must still write the IPsec rules to create the SA

Global settings



Global settings

Customize IPsec Settings

IPsec will use these settings to establish secured connections when there are active connection security rules or firewall rules that require authentication.

When you use the default, settings that have been specified at a higher precedence Group Policy object will be used.

Key exchange (Main Mode)

☒ Default (recommended)

☐ Advanced [Customize...](#)

Data protection (Quick Mode)

☒ Default (recommended)

☐ Advanced [Customize...](#)

Authentication Method

☒ Default

☐ Computer and User (using Kerberos V5)

☐ Computer (using Kerberos V5)

☐ User (using Kerberos V5)

☐ Computer certificate from this certification authority:

[Browse...](#)

☐ Accept only health certificates

☐ Advanced [Customize...](#)

[Learn more about IPsec settings](#)

[What are the default values?](#)

[OK](#) [Cancel](#)

Customize IPsec Settings

IPsec will use these settings to establish secured connections when there are active connection security rules or firewall rules that require authentication.

When you use the default, settings that have been specified at a higher precedence Group Policy object will be used.

Key exchange (Main Mode)

☐ Default (recommended)

☒ Advanced [Customize...](#)

Data protection (Quick Mode)

☐ Default (recommended)

☒ Advanced [Customize...](#)

Authentication Method

☐ Default

☐ Computer and User (using Kerberos V5)

☒ Computer (using Kerberos V5)

☐ User (using Kerberos V5)

☐ Computer certificate from this certification authority:

[Browse...](#)

☐ Accept only health certificates

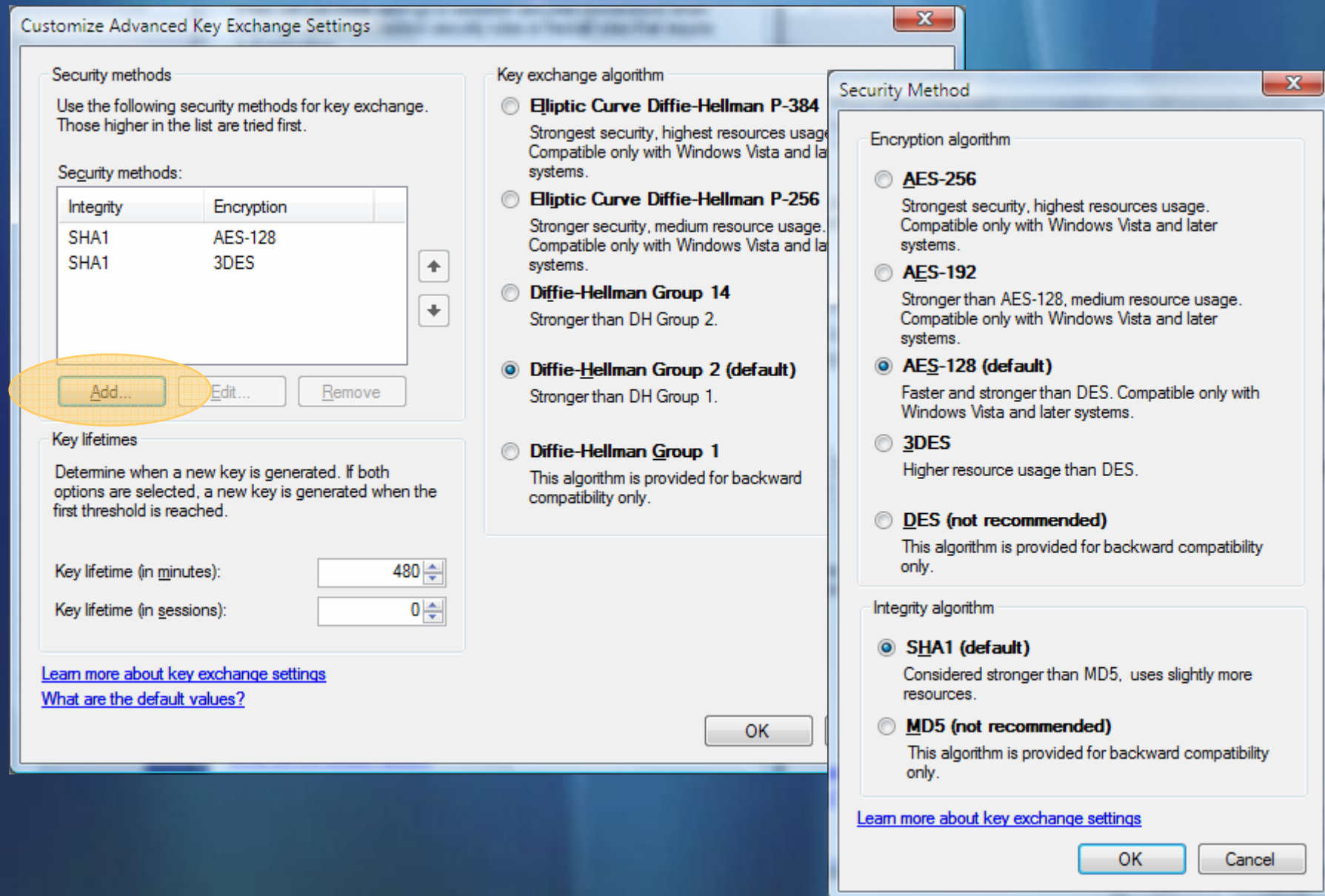
☒ Advanced [Customize...](#)

[Learn more about IPsec settings](#)

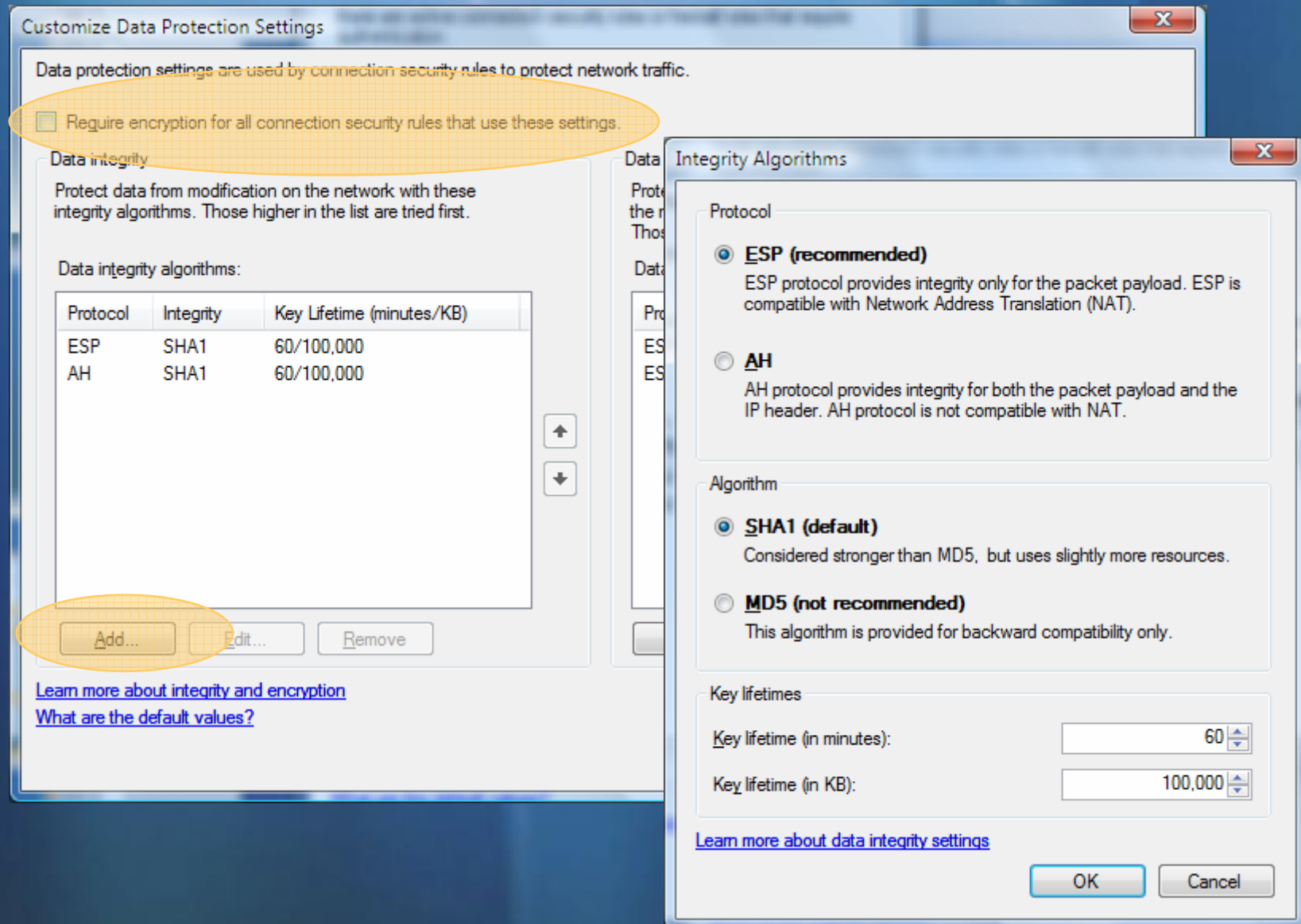
[What are the default values?](#)

[OK](#) [Cancel](#)

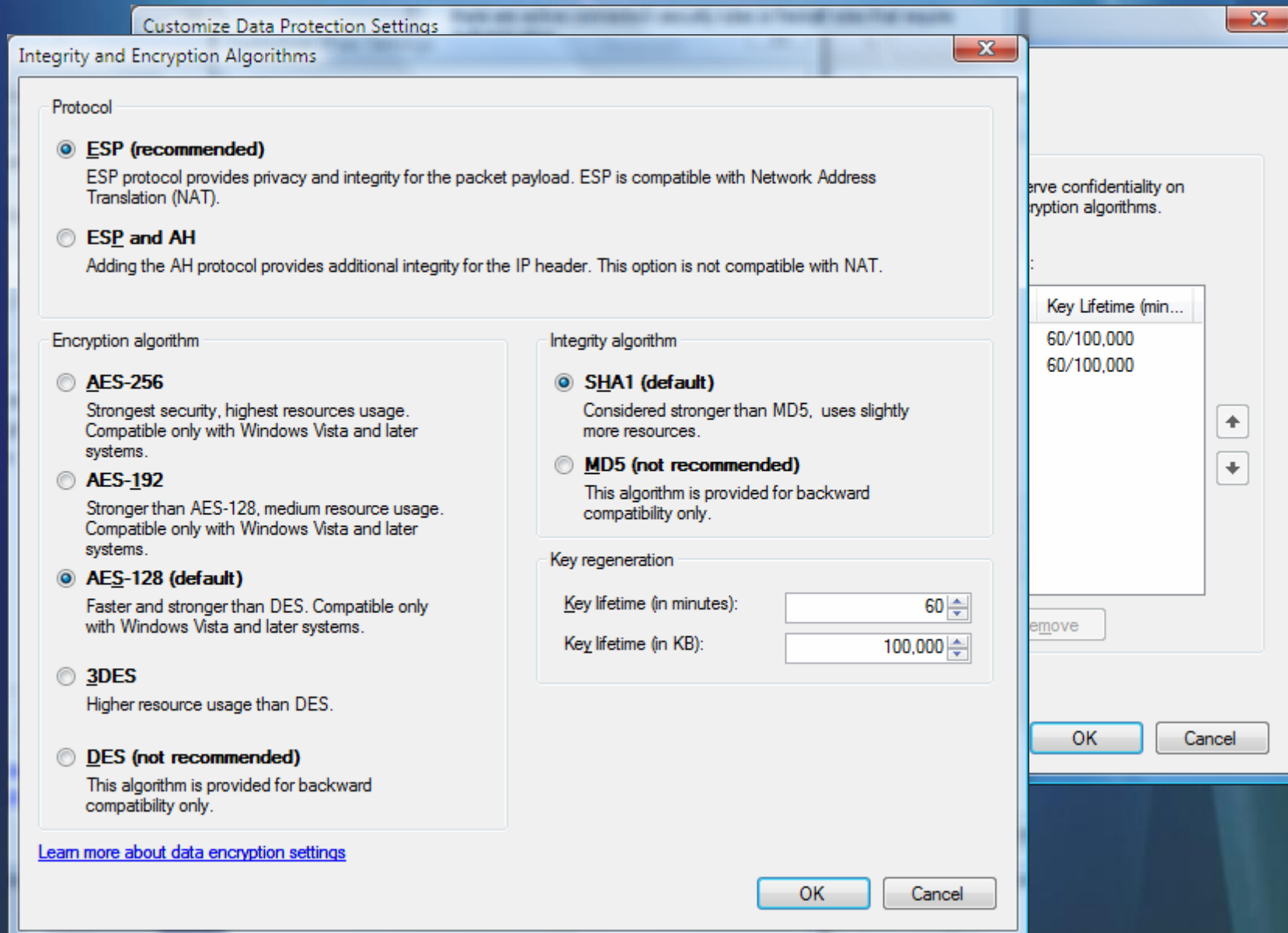
Global settings—key exchange (MM)



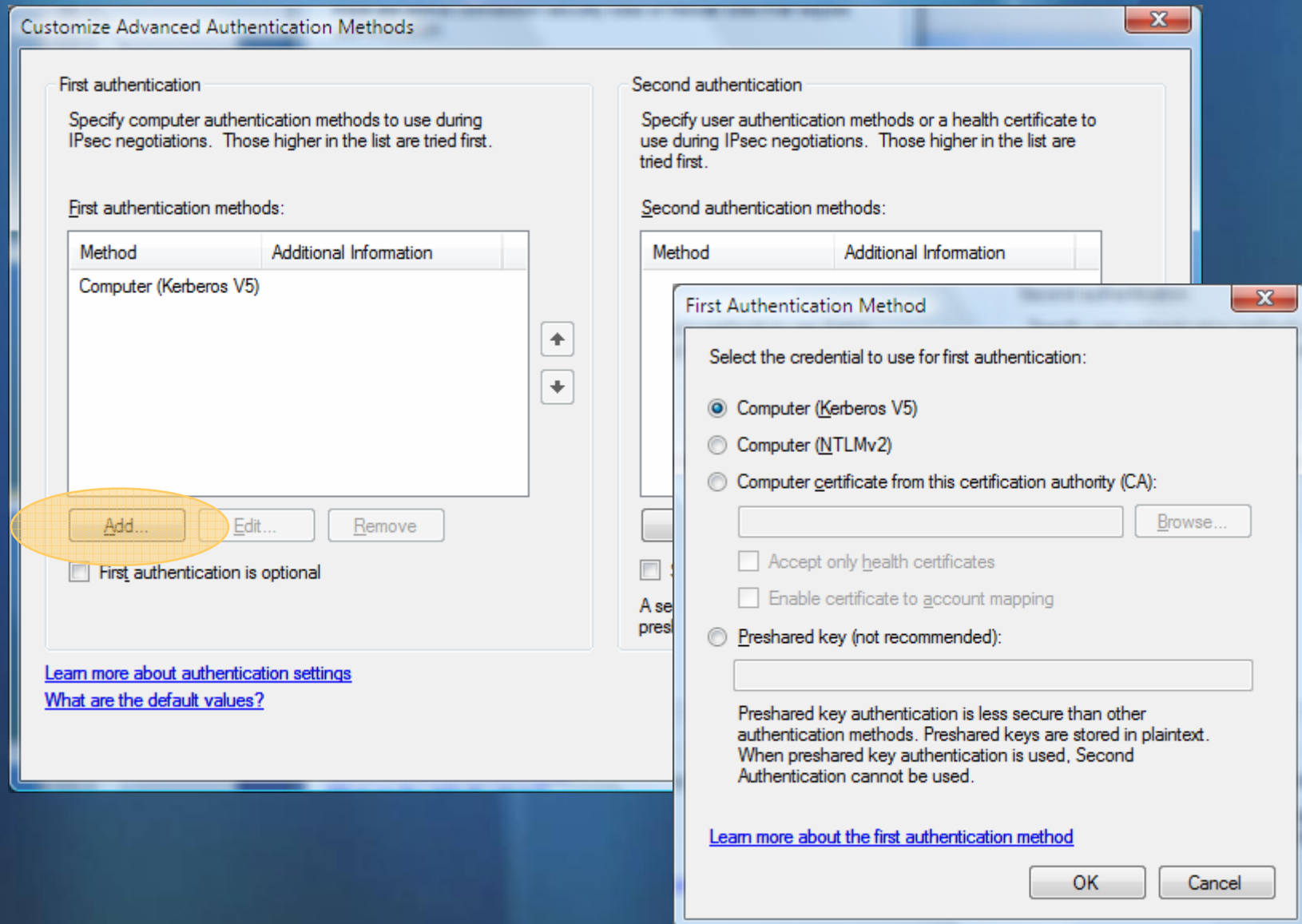
Global settings—data protection (QM)



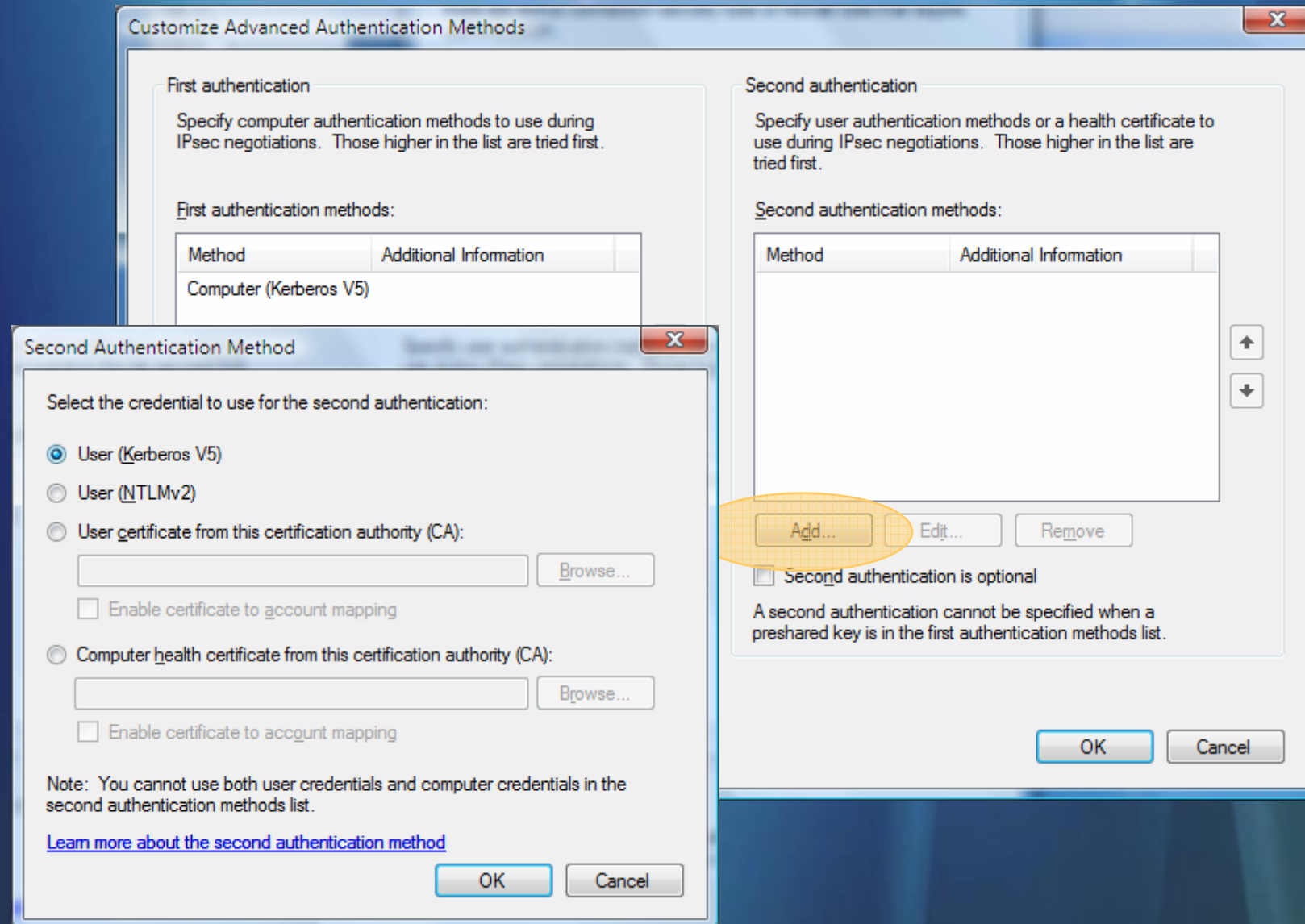
Global settings—data protection (QM)



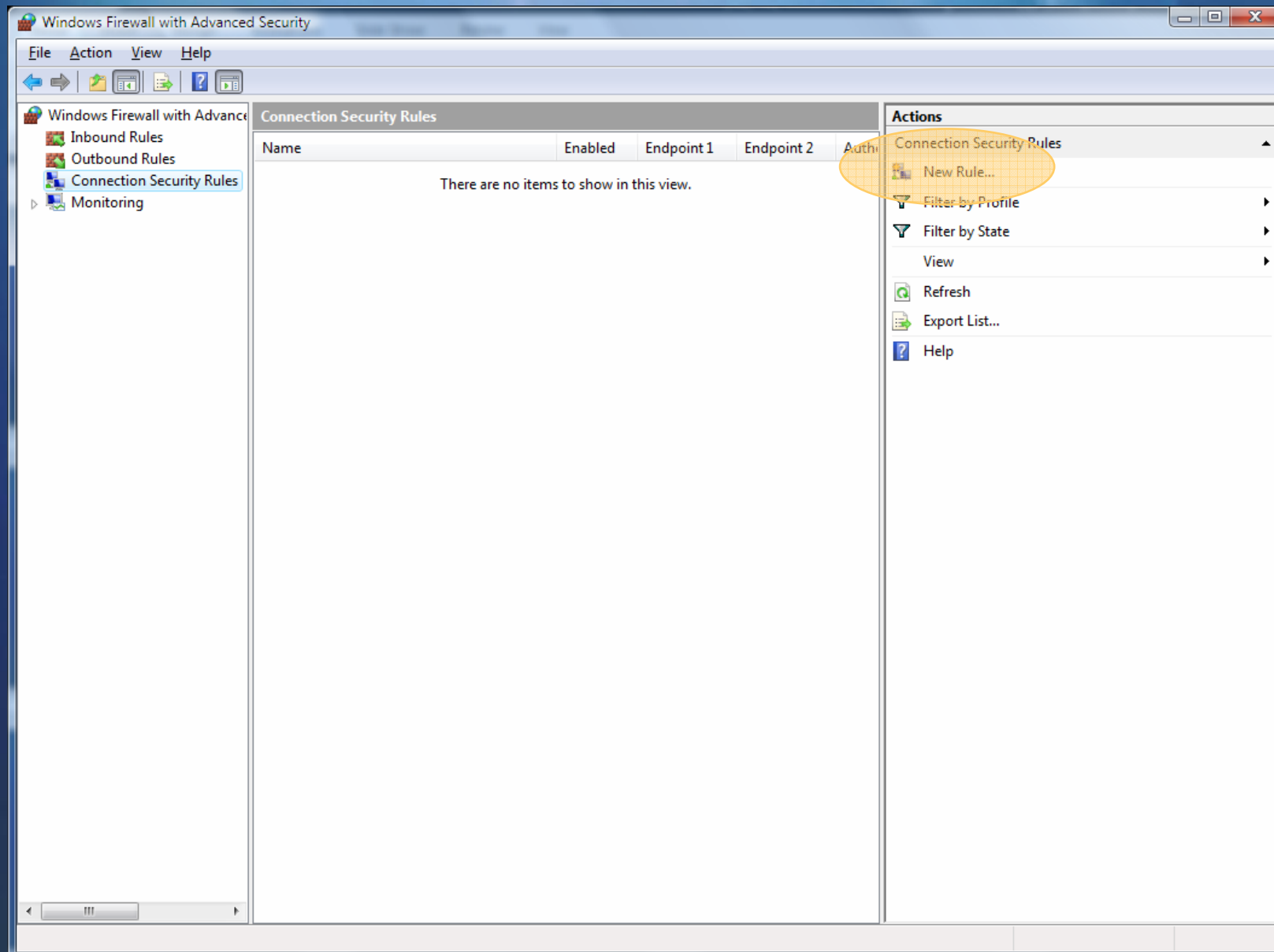
Global settings—authentication



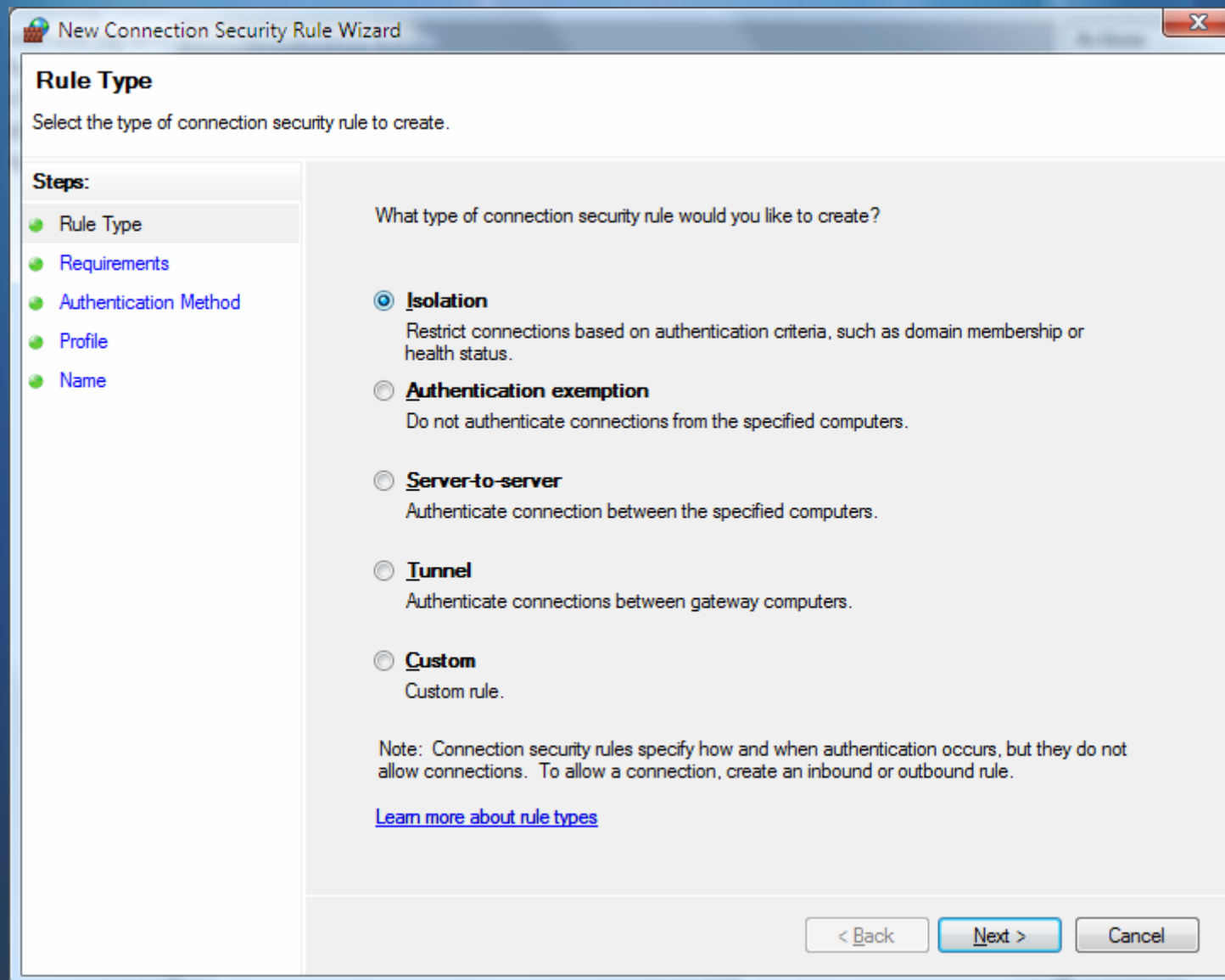
Global settings—authentication



Connection security rules



New rule



The image shows a Windows-style dialog box titled "New Connection Security Rule Wizard". It has a standard Windows window frame with a title bar, a close button (X), and a maximize button. The dialog is divided into two main sections. On the left is a "Steps:" pane with a list of steps: "Rule Type" (selected with a green dot), "Requirements", "Authentication Method", "Profile", and "Name". The main area on the right is titled "Rule Type" and contains the instruction "Select the type of connection security rule to create." Below this, it asks "What type of connection security rule would you like to create?". There are five radio button options: "Isolation" (selected), "Authentication exemption", "Server-to-server", "Tunnel", and "Custom". Each option has a brief description. At the bottom right are three buttons: "< Back", "Next >" (highlighted), and "Cancel". A note at the bottom of the main area explains that connection security rules specify authentication but do not allow connections, and provides a link to "Learn more about rule types".

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

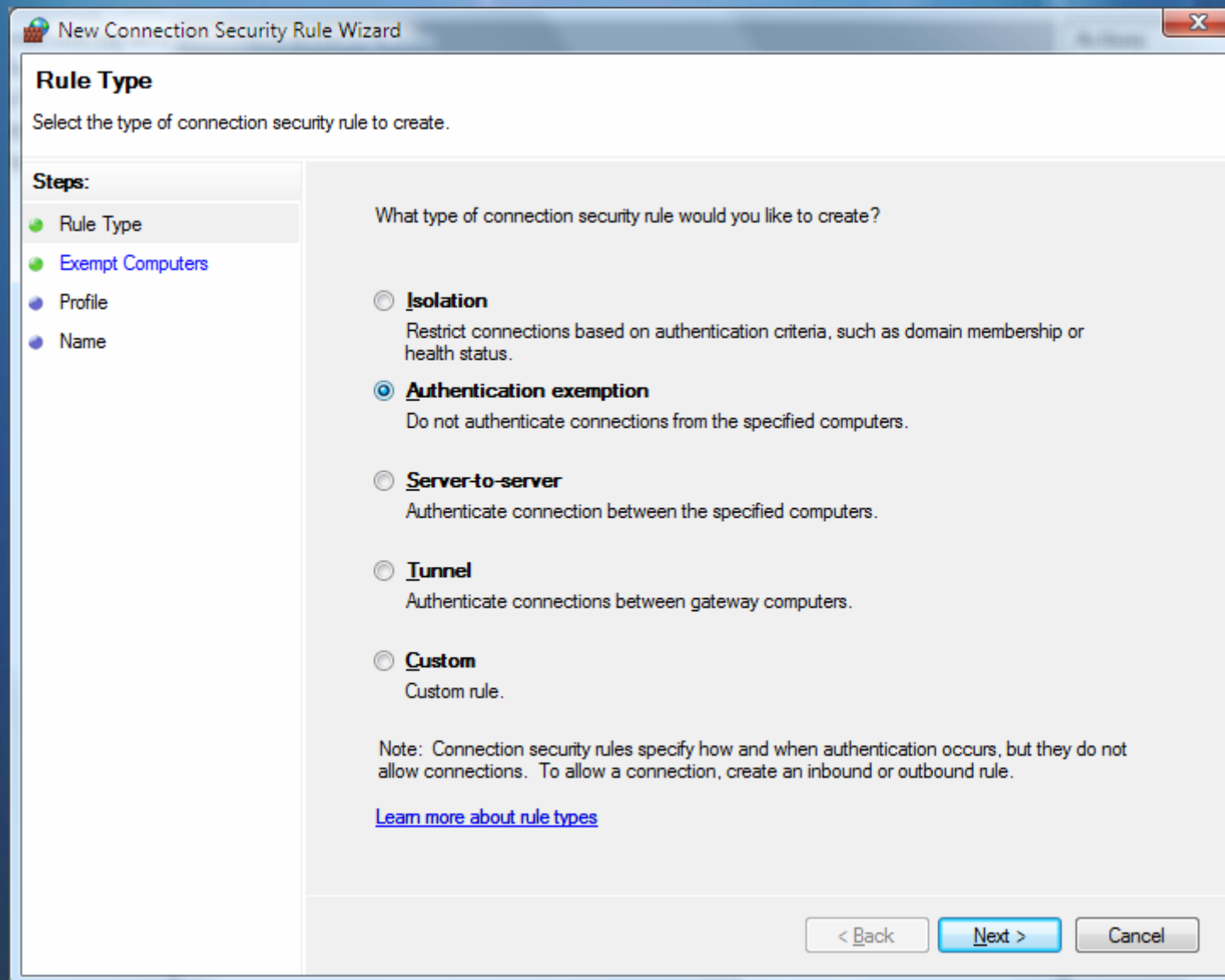
- ☒ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.
- ☐ **Authentication exemption**
Do not authenticate connections from the specified computers.
- ☐ **Server-to-server**
Authenticate connection between the specified computers.
- ☐ **Tunnel**
Authenticate connections between gateway computers.
- ☐ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

[Learn more about rule types](#)

< Back Next > Cancel

New rule



The image shows a Windows-style dialog box titled "New Connection Security Rule Wizard". It has a standard Windows window frame with a title bar, a close button (X), and a maximize button. The dialog is divided into two main sections. On the left is a "Steps:" pane with a list of four steps: "Rule Type" (selected with a green dot), "Exempt Computers" (green dot), "Profile" (blue dot), and "Name" (blue dot). The main area on the right is titled "Rule Type" and contains the instruction "Select the type of connection security rule to create." Below this, it asks "What type of connection security rule would you like to create?" and lists five radio button options: "Isolation" (restrict connections based on authentication criteria), "Authentication exemption" (selected, do not authenticate connections), "Server-to-server" (authenticate connection between specified computers), "Tunnel" (authenticate connections between gateway computers), and "Custom" (custom rule). At the bottom of the main area is a note: "Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule." and a link "Learn more about rule types". At the bottom right of the dialog are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Exempt Computers
- Profile
- Name

What type of connection security rule would you like to create?

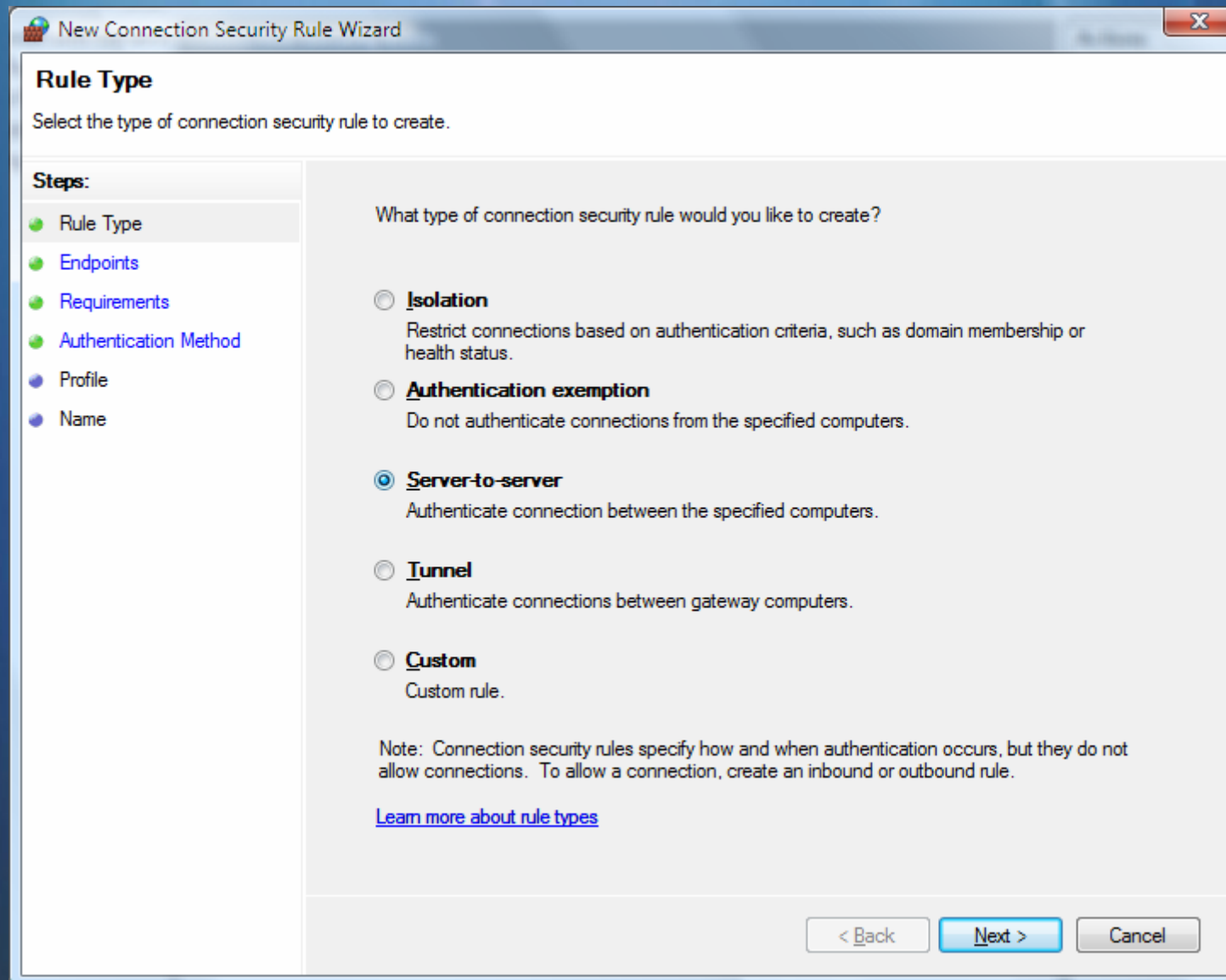
- ☐ **I**solation
Restrict connections based on authentication criteria, such as domain membership or health status.
- ☒ **A**uthentication exemption
Do not authenticate connections from the specified computers.
- ☐ **S**erver-to-server
Authenticate connection between the specified computers.
- ☐ **T**unnel
Authenticate connections between gateway computers.
- ☐ **C**ustom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

[Learn more about rule types](#)

< Back Next > Cancel

New rule



The image shows a Windows-style dialog box titled "New Connection Security Rule Wizard". It has a standard Windows window frame with a title bar, a close button (X), and a maximize button. The dialog is divided into two main sections. On the left is a "Steps:" pane with a list of steps: "Rule Type" (selected with a green dot), "Endpoints" (blue dot), "Requirements" (blue dot), "Authentication Method" (blue dot), "Profile" (blue dot), and "Name" (blue dot). The main area on the right is titled "Rule Type" and contains the instruction "Select the type of connection security rule to create." Below this, it asks "What type of connection security rule would you like to create?" and lists five options, each with a radio button: "Isolation" (restrict connections based on authentication criteria), "Authentication exemption" (do not authenticate connections), "Server-to-server" (selected, authenticate connection between specified computers), "Tunnel" (authenticate connections between gateway computers), and "Custom" (custom rule). At the bottom of the main area, there is a note: "Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule." and a link: "Learn more about rule types". At the bottom right of the dialog are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

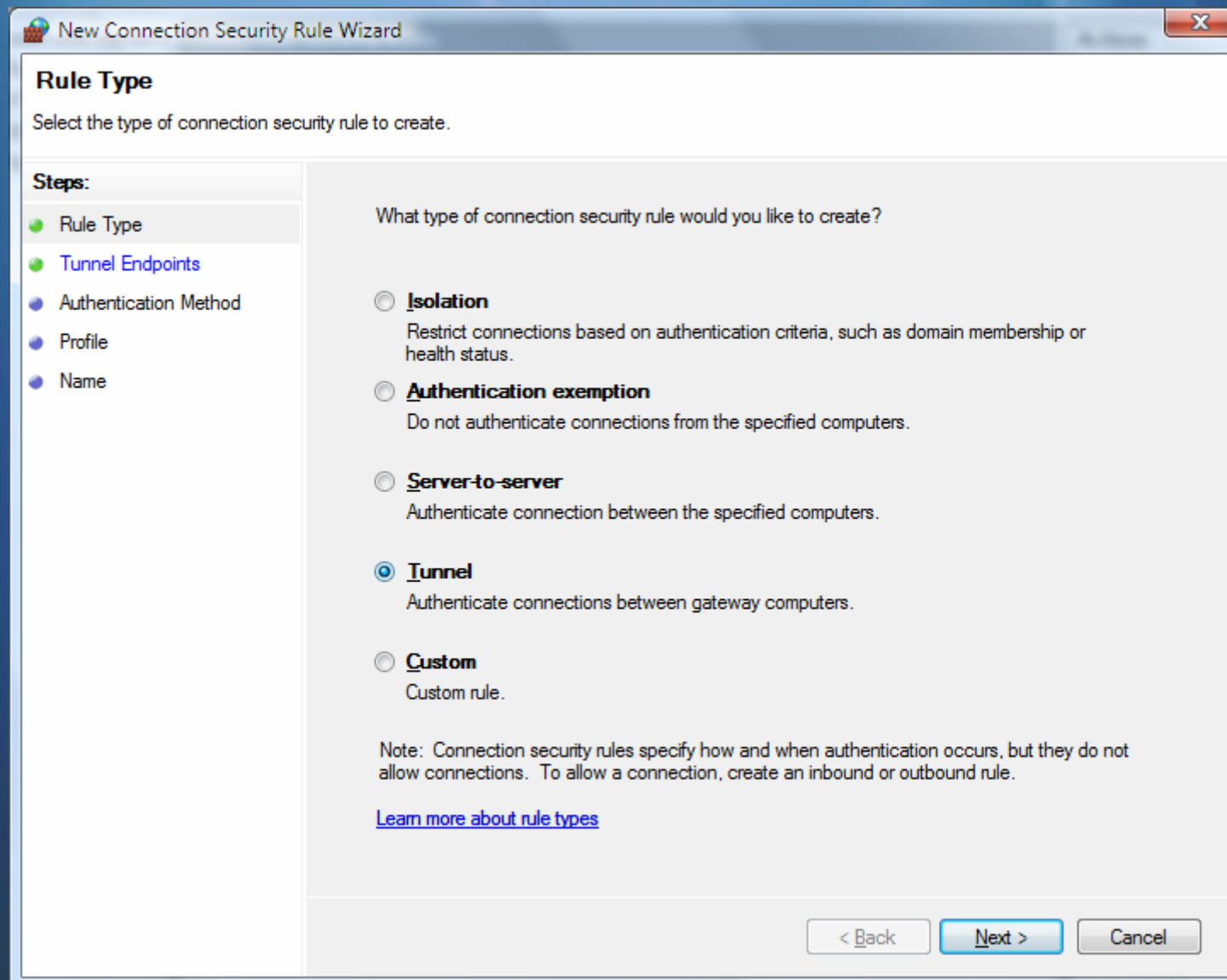
- ☐ **I**solation
Restrict connections based on authentication criteria, such as domain membership or health status.
- ☐ **A**uthentication exemption
Do not authenticate connections from the specified computers.
- ☒ **S**erver-to-server
Authenticate connection between the specified computers.
- ☐ **T**unnel
Authenticate connections between gateway computers.
- ☐ **C**ustom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

[Learn more about rule types](#)

< Back Next > Cancel

New rule



The image shows a Windows-style dialog box titled "New Connection Security Rule Wizard". It has a standard Windows window border with a title bar, a close button (X), and a "Back" button. The dialog is divided into two main sections. On the left is a "Steps:" pane with a list of five steps: "Rule Type" (highlighted with a green dot), "Tunnel Endpoints" (blue dot), "Authentication Method" (blue dot), "Profile" (blue dot), and "Name" (blue dot). The main area on the right is titled "Rule Type" and contains the instruction "Select the type of connection security rule to create." Below this, it asks "What type of connection security rule would you like to create?" and lists five radio button options: "Isolation" (restrict connections based on authentication criteria), "Authentication exemption" (do not authenticate connections from specified computers), "Server-to-server" (authenticate connection between specified computers), "Tunnel" (selected with a blue dot, authenticate connections between gateway computers), and "Custom" (custom rule). At the bottom of the main area, there is a note: "Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule." followed by a blue hyperlink "Learn more about rule types". At the bottom right of the dialog are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

- ☐ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.
- ☐ **Authentication exemption**
Do not authenticate connections from the specified computers.
- ☐ **Server-to-server**
Authenticate connection between the specified computers.
- ☒ **Tunnel**
Authenticate connections between gateway computers.
- ☐ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

[Learn more about rule types](#)

< Back Next > Cancel

New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

☐ **I**solation
Restrict connections based on authentication criteria, such as domain membership or health status.

☐ **A**uthentication exemption
Do not authenticate connections from the specified computers.

☐ **S**erver-to-server
Authenticate connection between the specified computers.

☐ **T**unnel
Authenticate connections between gateway computers.

☒ **C**ustom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

[Learn more about rule types](#)

< Back Next > Cancel

New rule—endpoints

New Connection Security Rule Wizard

Endpoints

Specify the computers between which secured connections will be established using IPsec.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Create a secured connection between computers in Endpoint 1 and Endpoint 2.

Which computers are in Endpoint 1?

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which computers are in Endpoint 2?

☒ Any IP address

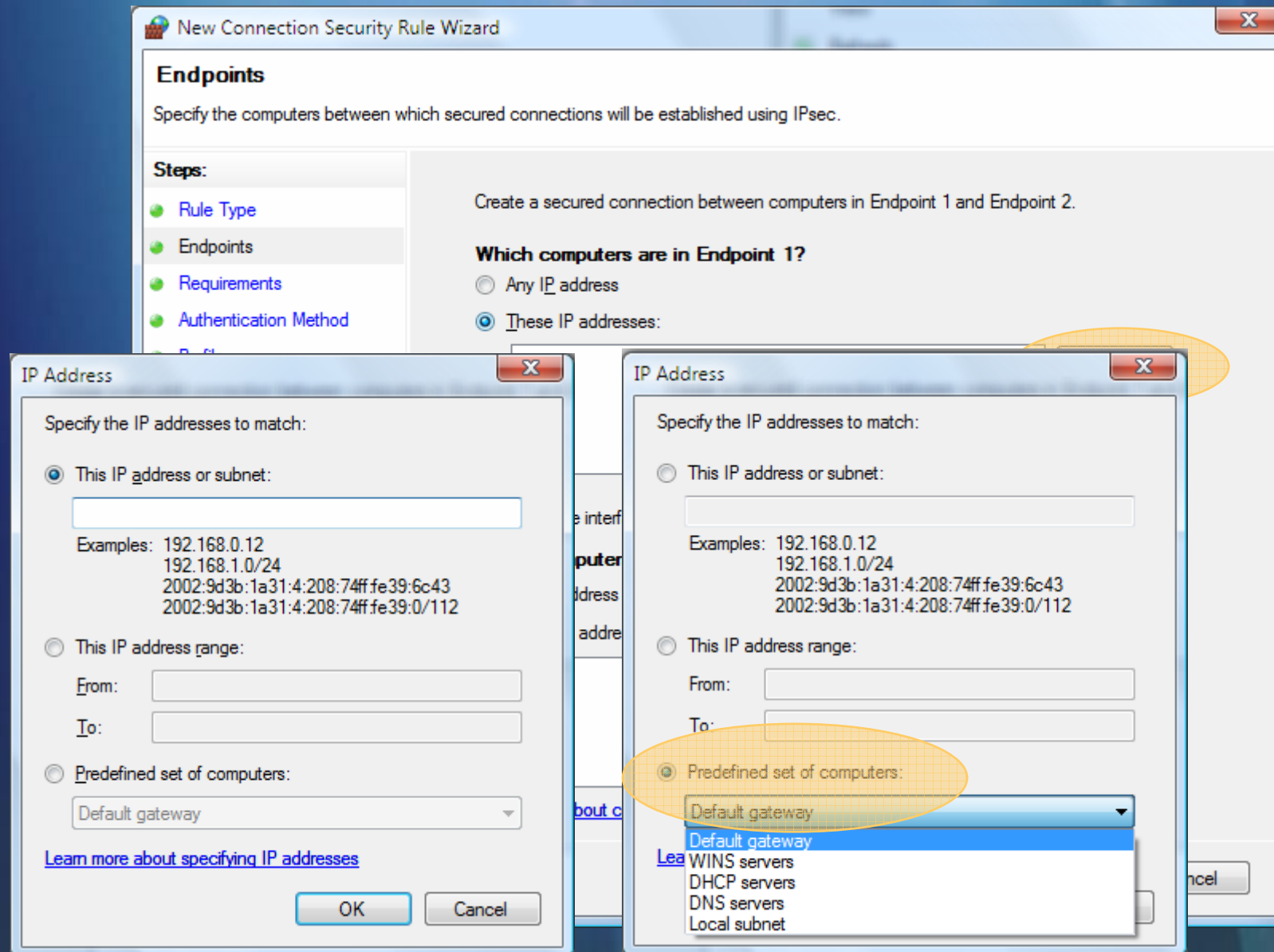
☐ These IP addresses:

Add... Edit... Remove

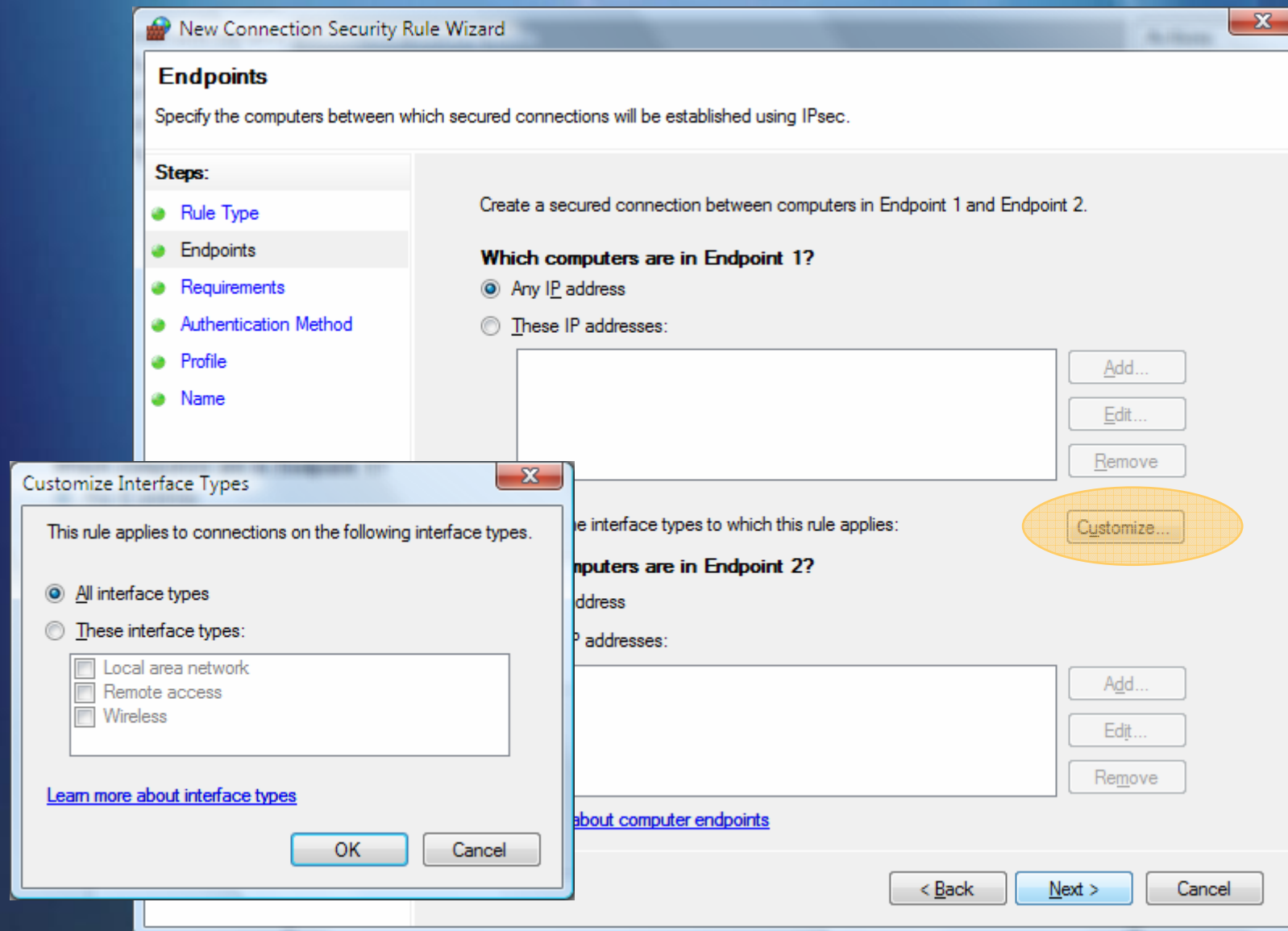
[Learn more about computer endpoints](#)

< Back Next > Cancel

New rule—endpoints



New rule—endpoints



New rule—tunnel endpoints

New Connection Security Rule Wizard

Tunnel Endpoints

Specify the endpoints for the IPsec tunnel defined by this rule.

Steps:

- Rule Type
- Tunnel Endpoints**
- Authentication Method
- Profile
- Name

Connections from Endpoint 1 to Endpoint 2 will pass through the specified tunnel endpoints. Tunnel endpoints are generally gateway servers.

Which computers are in Endpoint 1?

What is the local tunnel computer (closest to computers in Endpoint 1)?

IPv4 address:

IPv6 address:

What is the remote tunnel computer (closest to computers in Endpoint 2)?

IPv4 address:

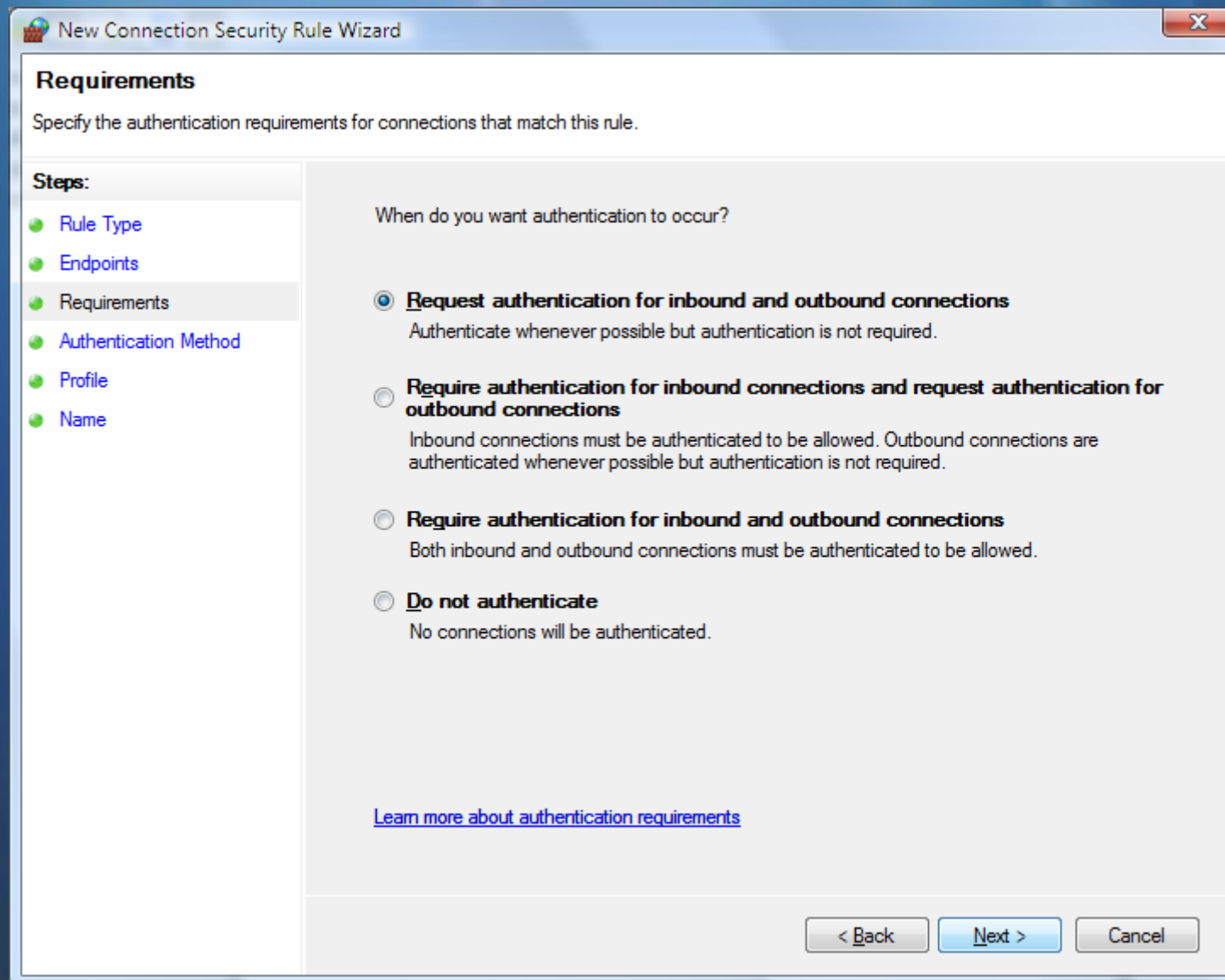
IPv6 address:

Which computers are in Endpoint 2?

[Learn more about tunnel endpoints](#)

< Back Next > Cancel

New rule—requirements



The image shows a screenshot of the 'New Connection Security Rule Wizard' window, specifically the 'Requirements' step. The window has a title bar with the text 'New Connection Security Rule Wizard' and a close button. The main area is titled 'Requirements' and contains the instruction 'Specify the authentication requirements for connections that match this rule.' On the left, there is a 'Steps:' list with six items: 'Rule Type', 'Endpoints', 'Requirements' (which is selected and highlighted), 'Authentication Method', 'Profile', and 'Name'. The main content area asks 'When do you want authentication to occur?' and provides four radio button options: 1. 'Request authentication for inbound and outbound connections' (selected), with the description 'Authenticate whenever possible but authentication is not required.' 2. 'Require authentication for inbound connections and request authentication for outbound connections', with the description 'Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.' 3. 'Require authentication for inbound and outbound connections', with the description 'Both inbound and outbound connections must be authenticated to be allowed.' 4. 'Do not authenticate', with the description 'No connections will be authenticated.' At the bottom of the main area is a blue hyperlink: 'Learn more about authentication requirements'. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements**
- Authentication Method
- Profile
- Name

When do you want authentication to occur?

- ☒ **Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.
- ☐ **Require authentication for inbound connections and request authentication for outbound connections**
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.
- ☐ **Require authentication for inbound and outbound connections**
Both inbound and outbound connections must be authenticated to be allowed.
- ☐ **Do not authenticate**
No connections will be authenticated.

[Learn more about authentication requirements](#)

< Back Next > Cancel

New rule—authentication

New Connection Security Rule Wizard

Authentication Method

Specify how authentication is performed for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method**
- Profile
- Name

What authentication method would you like to use?

☒ **Default**
Use the authentication methods specified in the profile properties.

☐ **Computer and user (Kerberos V5)**
Restrict communications to connections from domain-joined users and computers. Provides identity information for authorizing specific users and computers in inbound and outbound rules.

☐ **Computer (Kerberos V5)**
Restrict communications to connections from domain-joined computers. Provides identity information for authorizing specific computers in inbound and outbound rules.

☐ **Computer certificate**
Restrict communications to connections from computers that have a certificate from this certification authority (CA).
CA name:
☐ Only accept health certificates

☐ **Advanced**
Specify custom first and second authentication settings.

[Learn more about authentication methods](#)

< Back Next > Cancel

New rule—authentication

Customize Advanced Authentication Methods

First authentication
Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
--------	------------------------

↑
↓

Add... Edit... Remove

☐ First authentication is optional

Second authentication
Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first.

Second authentication methods:

Method	Additional Information
--------	------------------------

↑
↓

Add... Edit... Remove

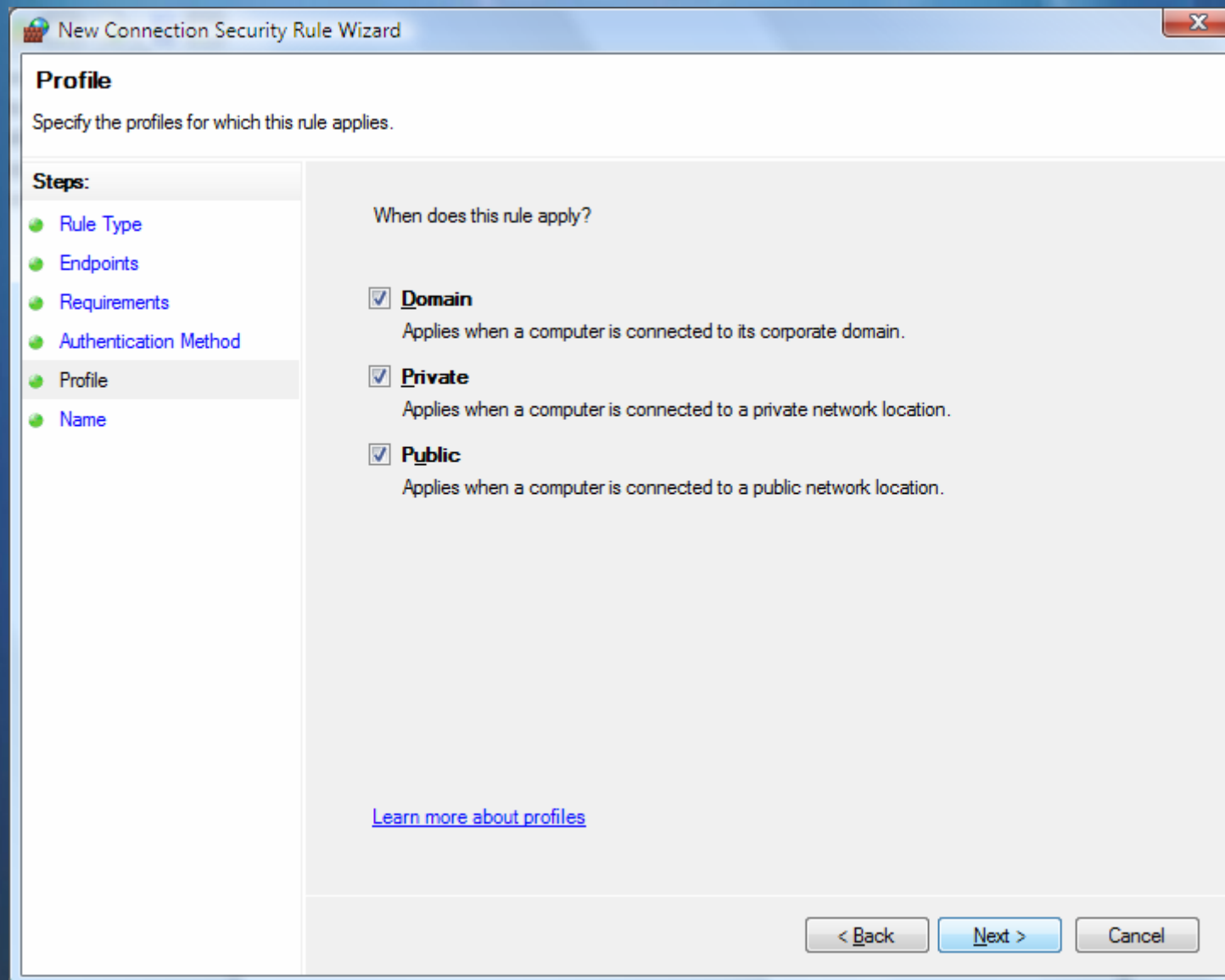
☐ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

[Learn more about authentication settings](#)
[What are the default values?](#)

OK Cancel

New rule—profile



The image shows a screenshot of the 'New Connection Security Rule Wizard' window, specifically the 'Profile' step. The window has a title bar with the text 'New Connection Security Rule Wizard' and a close button. The main content area is titled 'Profile' and contains the instruction 'Specify the profiles for which this rule applies.' On the left side, there is a 'Steps:' list with the following items: 'Rule Type', 'Endpoints', 'Requirements', 'Authentication Method', 'Profile' (which is highlighted), and 'Name'. The main area on the right is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom of the main area, there is a link that says 'Learn more about profiles'. At the bottom right of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile**
- Name

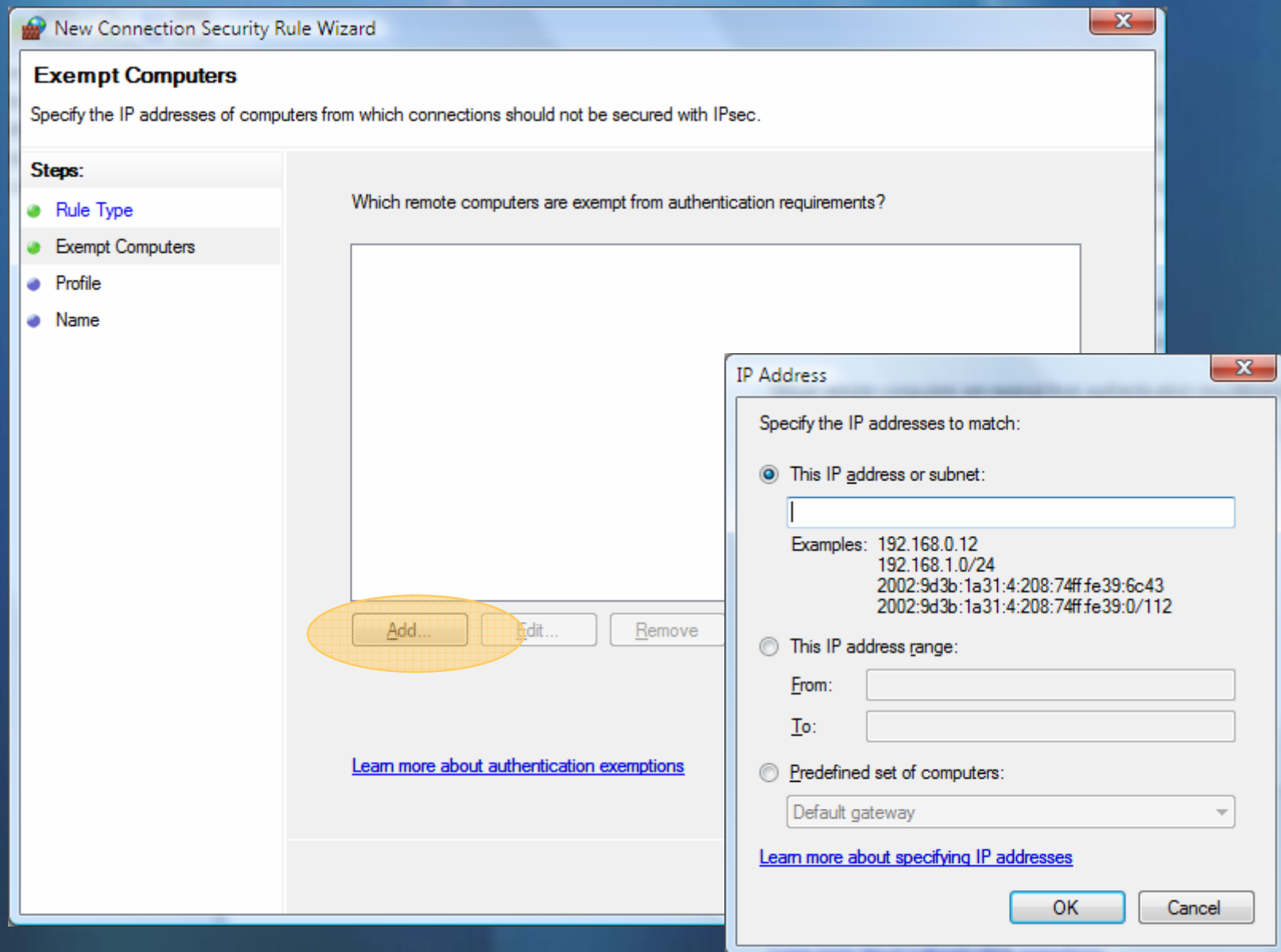
When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location.
- ☒ **Public**
Applies when a computer is connected to a public network location.

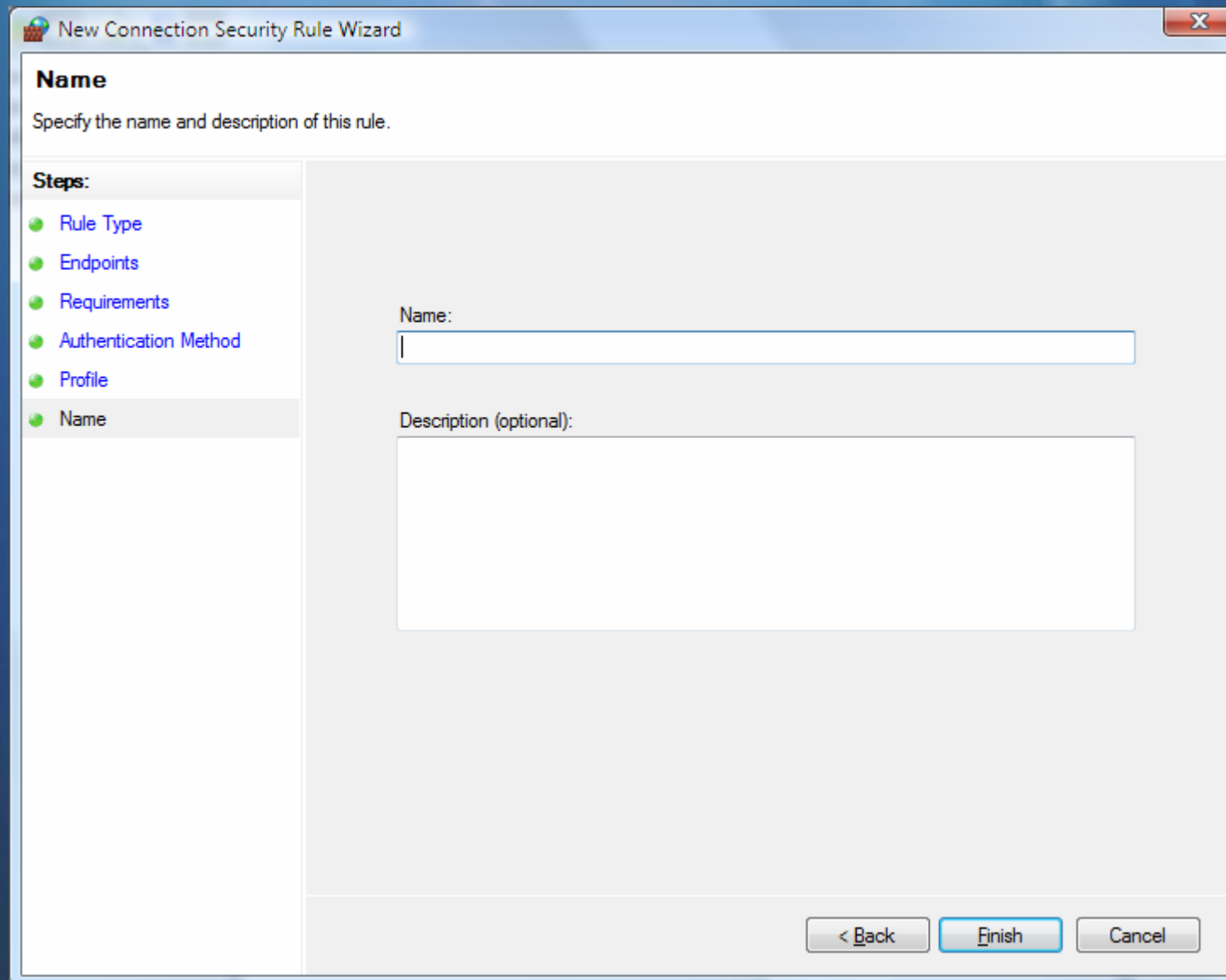
[Learn more about profiles](#)

< Back Next > Cancel

New rule—exemptions



New rule—name



The image shows a Windows-style dialog box titled "New Connection Security Rule Wizard". The window has a standard title bar with a close button (X) in the top right corner. The main content area is divided into two sections. On the left, there is a "Steps:" list with six items, each preceded by a green circular icon: "Rule Type", "Endpoints", "Requirements", "Authentication Method", "Profile", and "Name". The "Name" step is currently selected and highlighted with a light gray background. To the right of this list, the main area is titled "Name" and contains the instruction "Specify the name and description of this rule." Below this instruction, there are two input fields: a single-line text box labeled "Name:" and a larger multi-line text box labeled "Description (optional):". At the bottom right of the dialog, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a blue border.

New Connection Security Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Name:

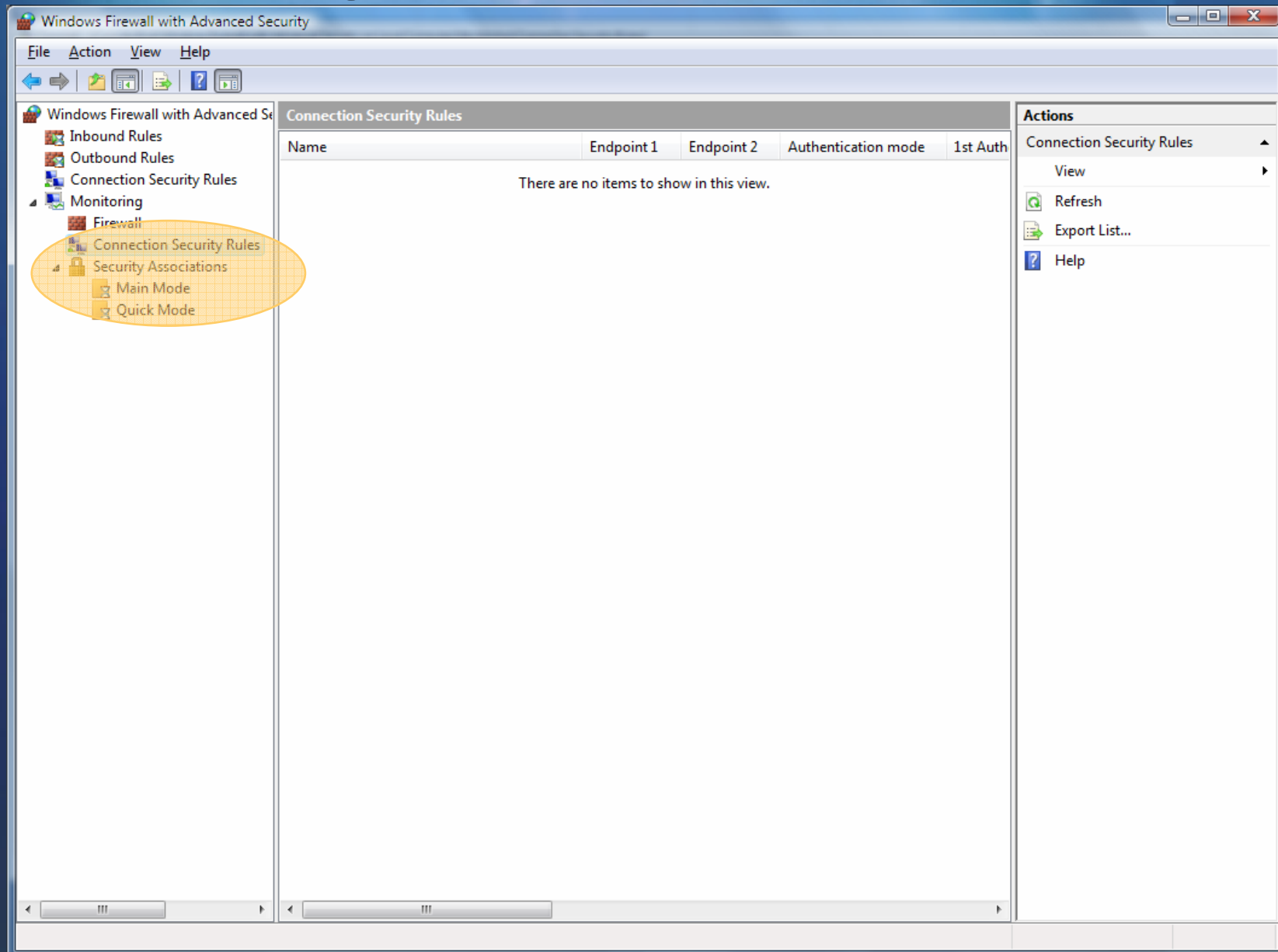
Description (optional):


< Back Finish Cancel

IPsec auditing and diagnostics

- Added 15 new IPsec audit-specific events and 20 new firewall events
- 25 legacy event texts rewritten to reflect a more accurate state
- No more generic events
- Implemented granular control of the IPsec audit policy (3 main categories with 8 sub categories)
- Events include all the information needed for troubleshooting; no tracing required
- Oakley log replaced with WPP tracing (intended for Microsoft internal use only)
- Defined different logical Perfmon counters sets (IKE4, IKEv6, AUTHIPv4, AuthIPv6, ...)
- Overall added 150 new Perfmon counters between IPsec and firewall
- Improved IPsecmon—event texts include troubleshooting hints
- Integrated with NetXP, an end-user tool for diagnosing and resolving connection problems

Monitoring



The background is a deep blue gradient with several bright, diagonal light rays emanating from the top right. The left and right edges of the image are styled to look like torn paper, with irregular white shapes cut out. Two thin, horizontal light blue lines are positioned above and below the main text.

But I'm Not Running Vista Yet

You've got a firewall already

- Switch it on.
- Now.
- Without delay.
- Did I mention the urgency?
- I use it ☺



Steve Riley
steve.riley@microsoft.com
<http://blogs.technet.com/steriley>



www.protectyourwindowsnetwork.com

Thanks very much!

Microsoft®

Your potential. Our passion.™

© 2006 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.