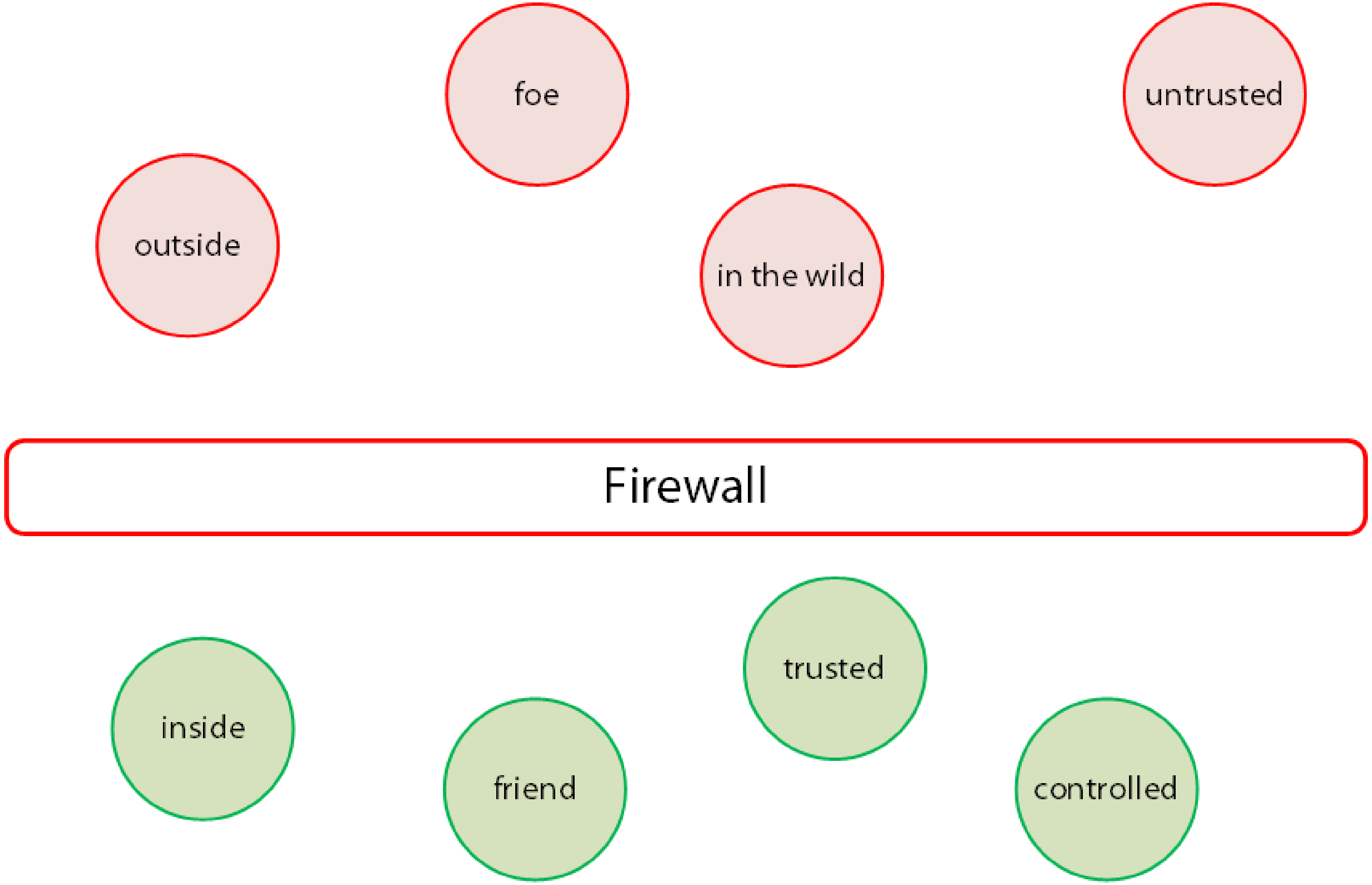
system.de

Die Service Manufaktur der digitalen Transformation

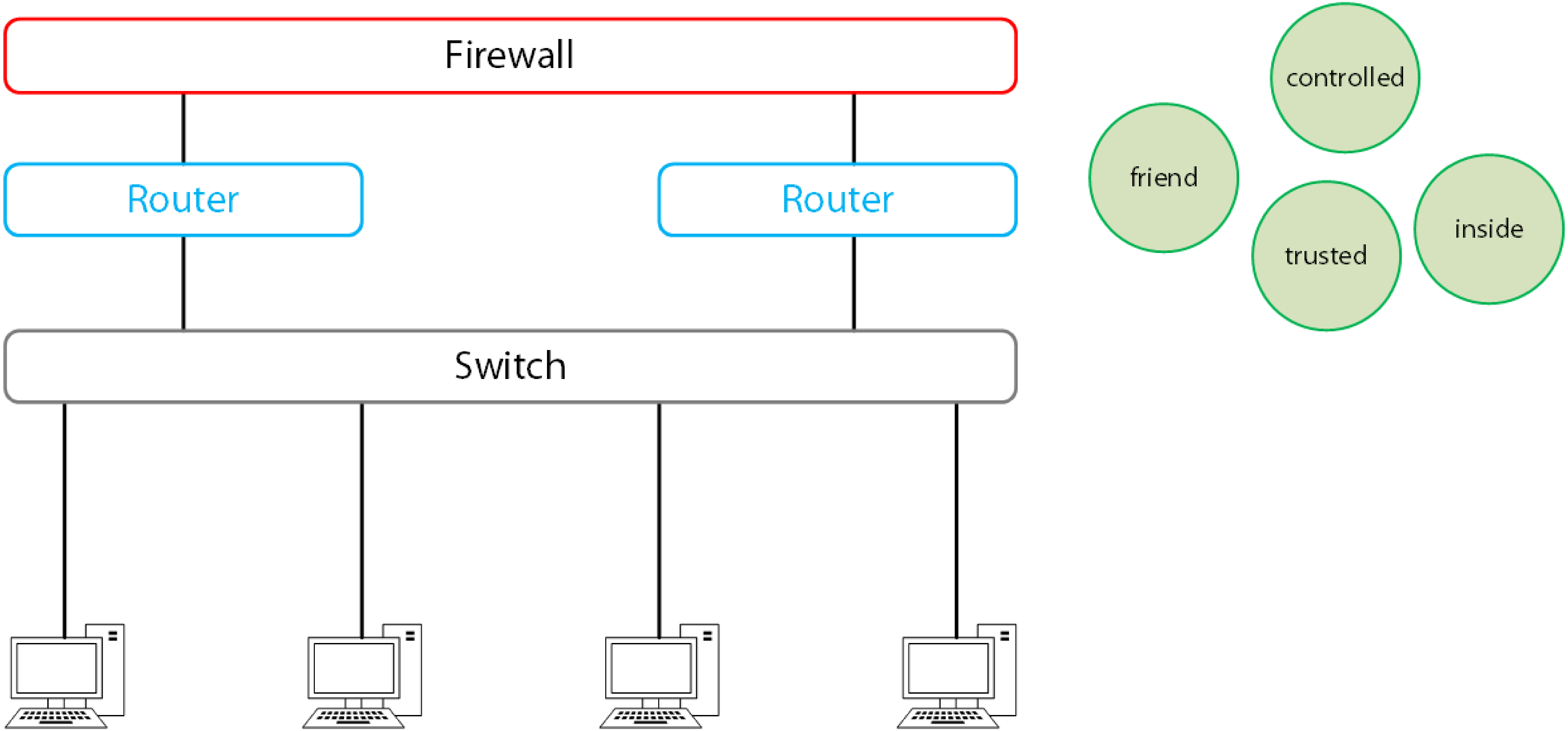
IPv6 and the Windows 10 Firewall

Firewall?

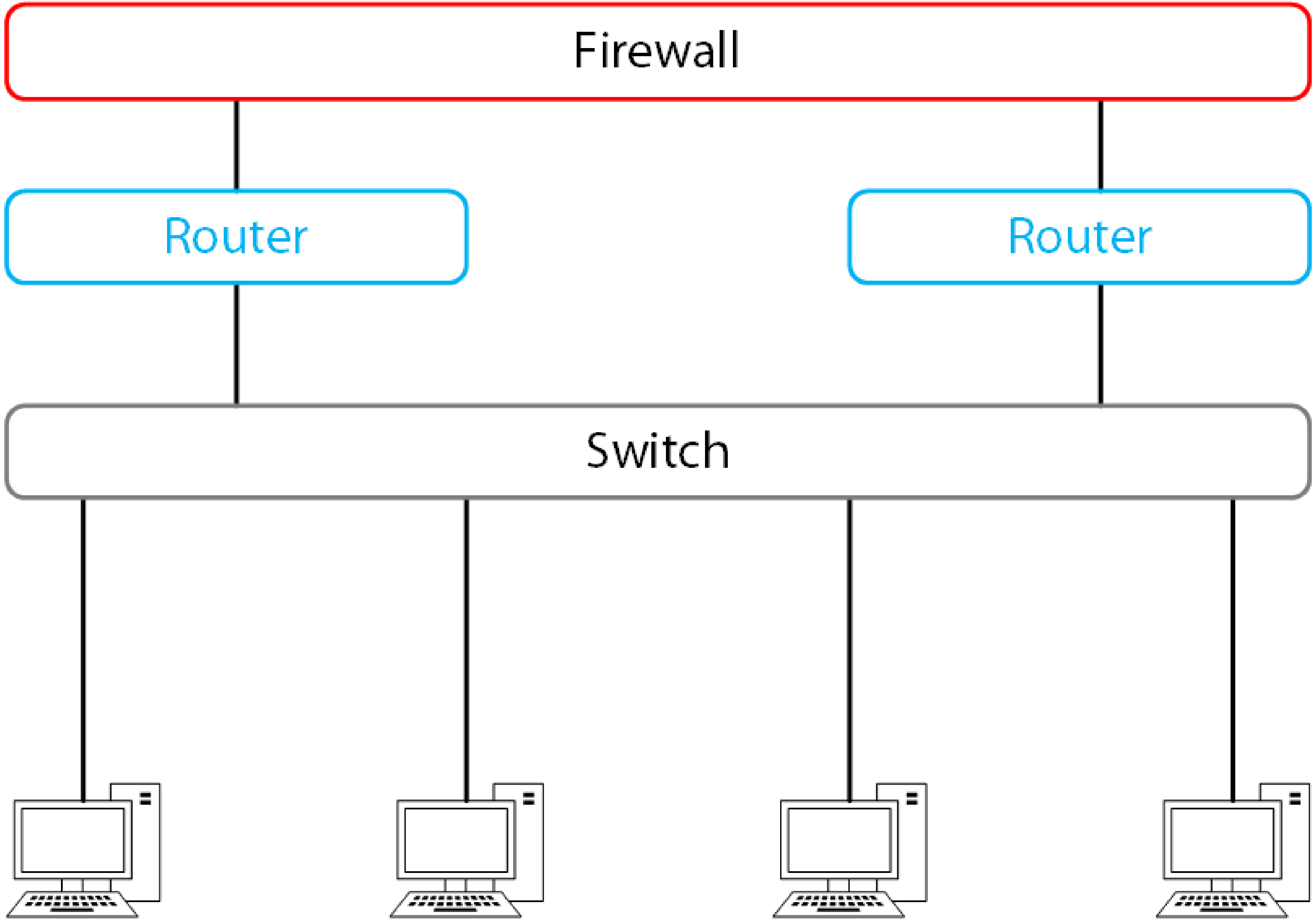
Network Firewall

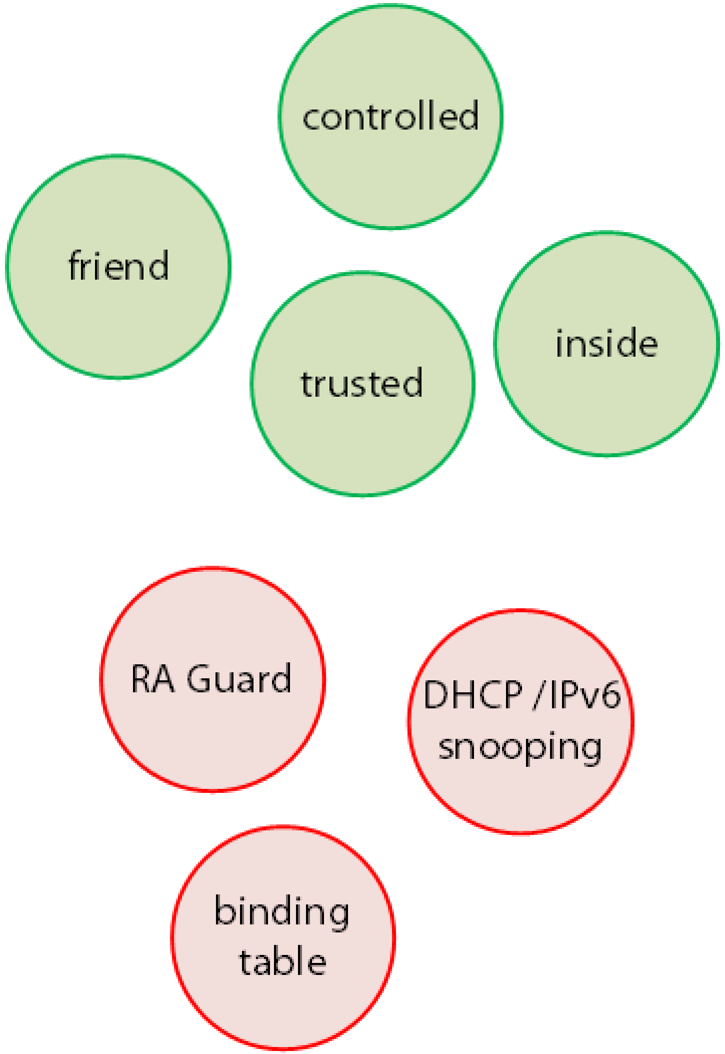


IPv6 in the LAN



IPv6 in the LAN





Windows 10 Firewall

Use of Profiles

Private

Public

Domain

image: Flaticon.com

Three Profiles

- Public
- Private
- Domain

Three Sources

- Local Rules
- AD Server / Group Policy
- Both

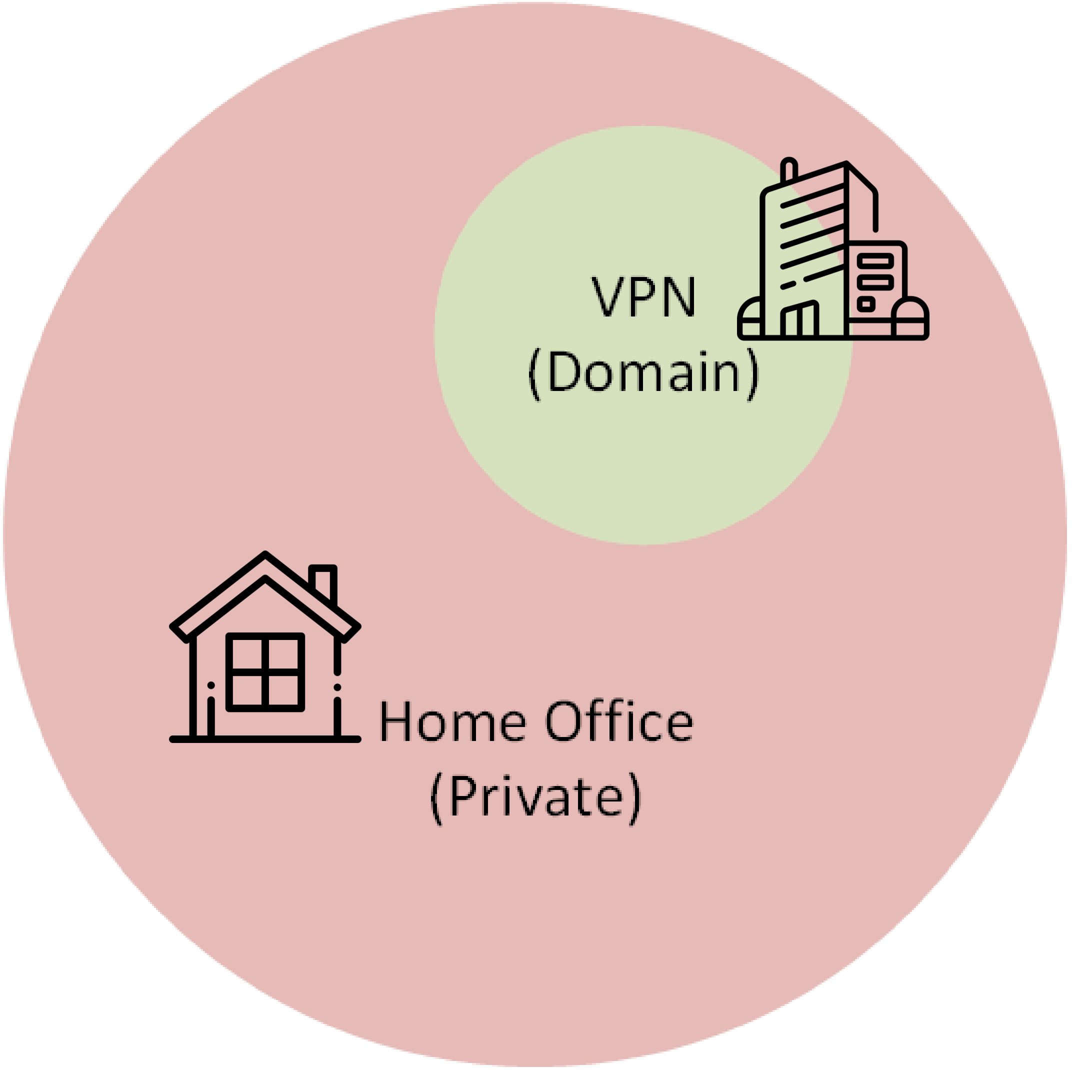
Use of Profiles today (Home Office)

- Two profiles are commonly used

- VPN ruleset from enterprise

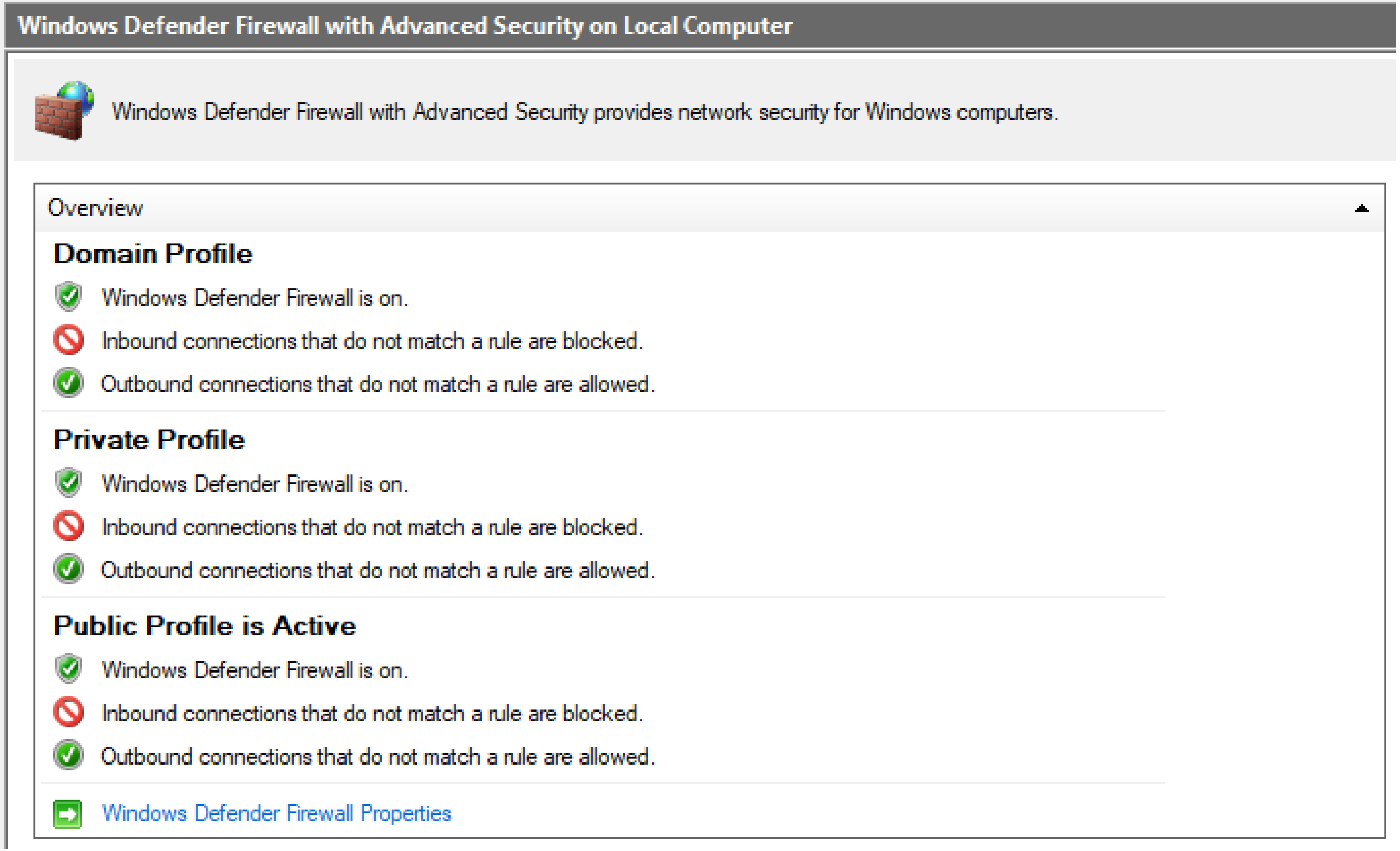
- Home network ruleset by Microsoft

- Two rulesets
- Two sources
- Two admins responsible



IPv6 Ruleset

Default Behavior



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

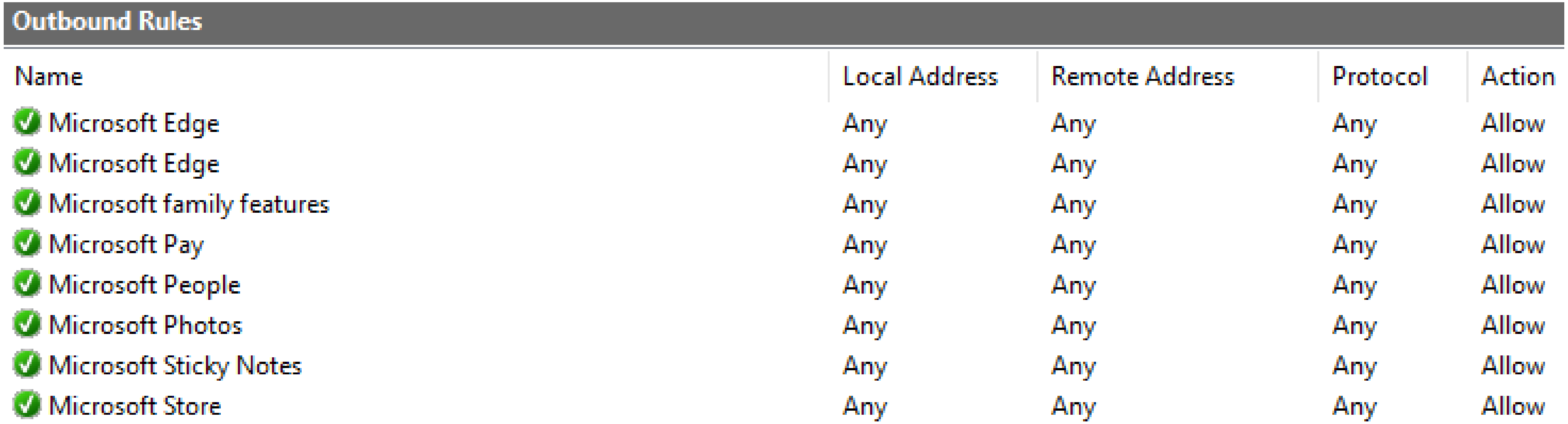
✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Firewall for Services

- Many rules are for services / applications
- Rules apply to IPv4 and IPv6

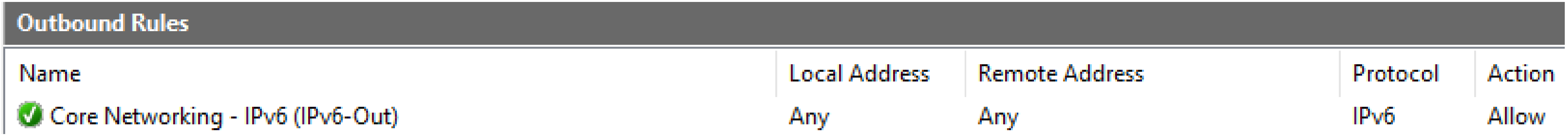
- Plan your rules accordingly
- Mircosoft firewall is a host firewall



Outbound Rules

Name	Local Address	Remote Address	Protocol	Action
✓ Microsoft Edge	Any	Any	Any	Allow
✓ Microsoft Edge	Any	Any	Any	Allow
✓ Microsoft family features	Any	Any	Any	Allow
✓ Microsoft Pay	Any	Any	Any	Allow
✓ Microsoft People	Any	Any	Any	Allow
✓ Microsoft Photos	Any	Any	Any	Allow
✓ Microsoft Sticky Notes	Any	Any	Any	Allow
✓ Microsoft Store	Any	Any	Any	Allow

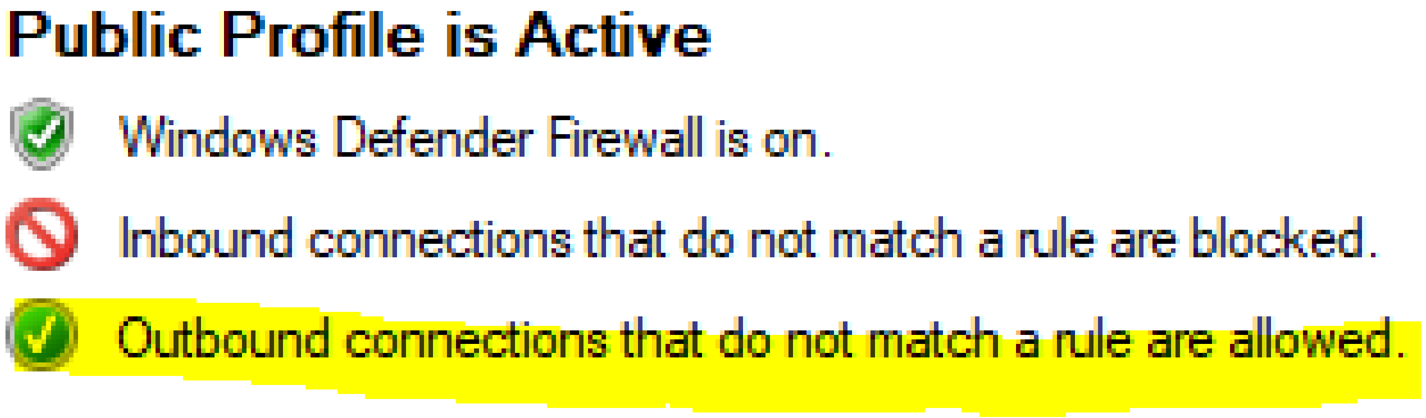
IPv6 outbound



Outbound Rules

Name	Local Address	Remote Address	Protocol	Action
✓ Core Networking - IPv6 (IPv6-Out)	Any	Any	IPv6	Allow

- IPv6 outbound is allowed



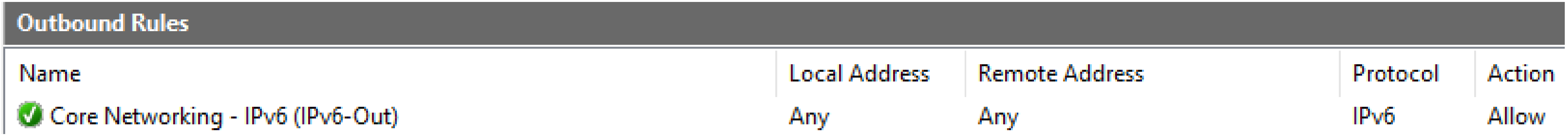
Public Profile is Active

✓ Windows Defender Firewall is on.

🛇 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

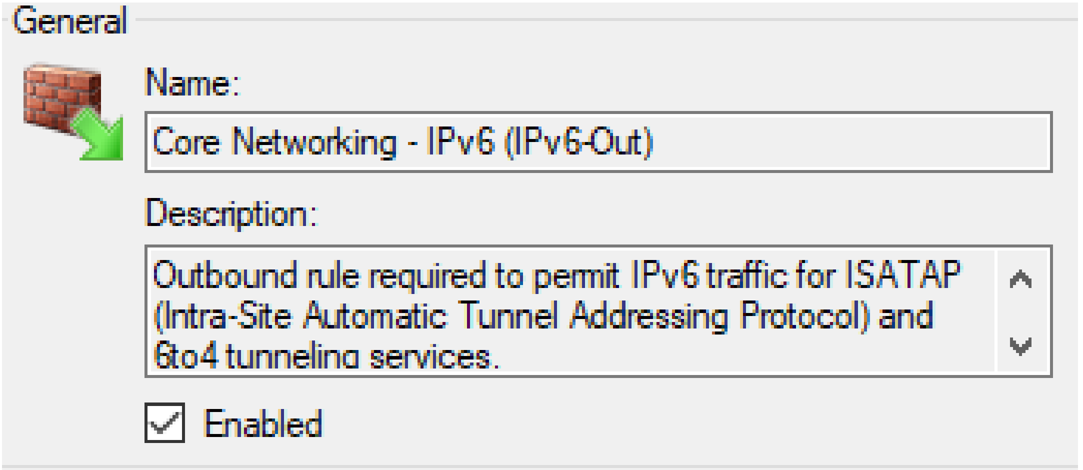
IPv6 outbound



Outbound Rules

Name	Local Address	Remote Address	Protocol	Action
✓ Core Networking - IPv6 (IPv6-Out)	Any	Any	IPv6	Allow

- IPv6 outbound is allowed



General

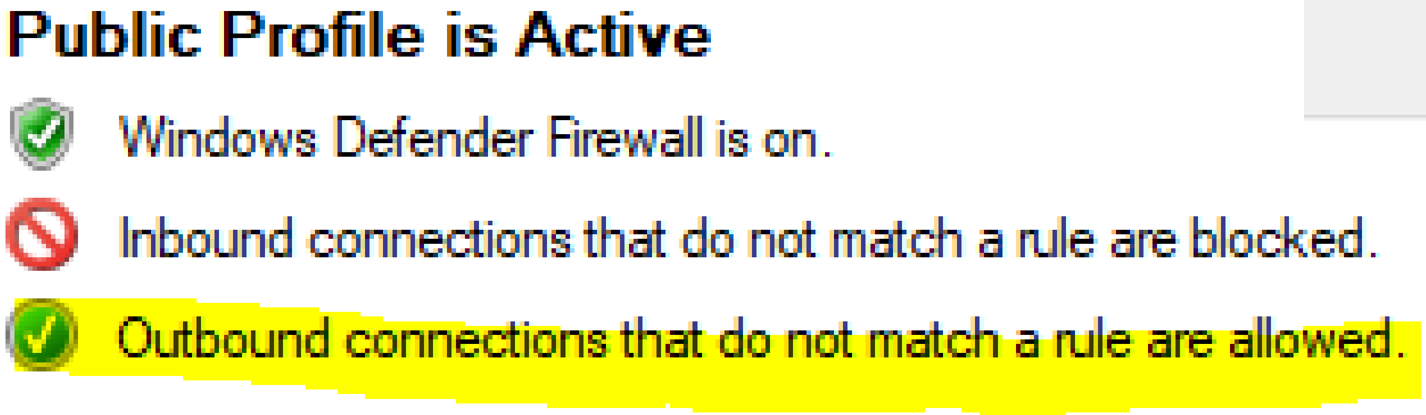
Name:

Core Networking - IPv6 (IPv6-Out)

Description:

Outbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.

☑ Enabled



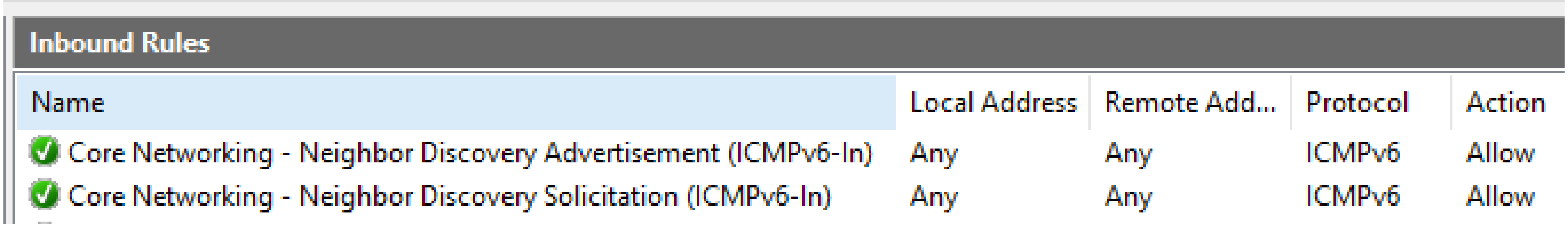
Public Profile is Active

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

IPv6 inbound

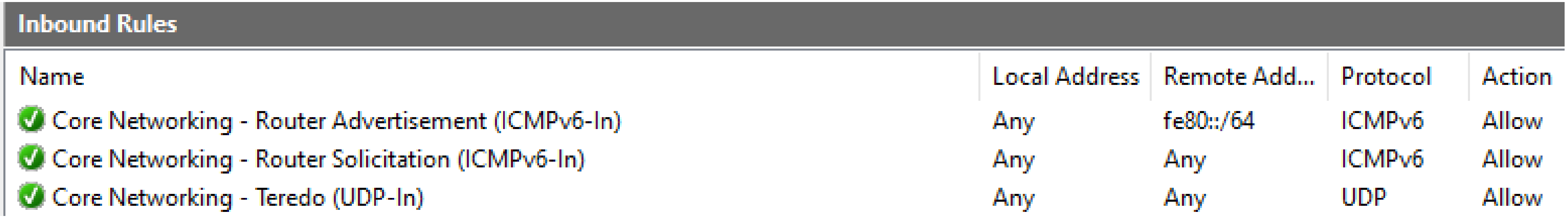


Inbound Rules

Name	Local Address	Remote Add...	Protocol	Action
✓ Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	Any	Any	ICMPv6	Allow
✓ Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	Any	Any	ICMPv6	Allow

- Neighbor discovery has to reach our computer

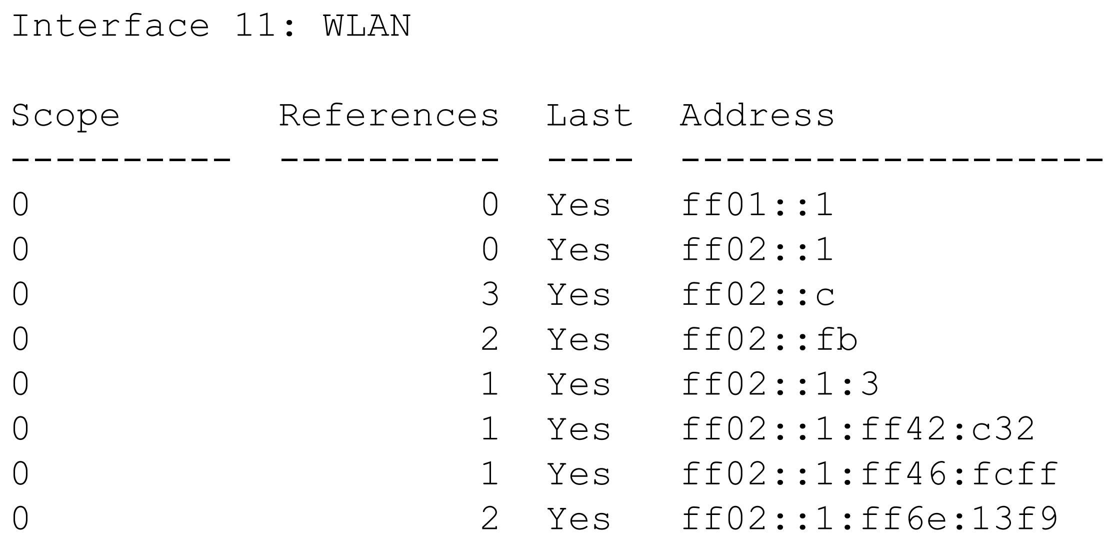
IPv6 inbound



Inbound Rules

Name	Local Address	Remote Add...	Protocol	Action
✓ Core Networking - Router Advertisement (ICMPv6-In)	Any	fe80::/64	ICMPv6	Allow
✓ Core Networking - Router Solicitation (ICMPv6-In)	Any	Any	ICMPv6	Allow
✓ Core Networking - Teredo (UDP-In)	Any	Any	UDP	Allow

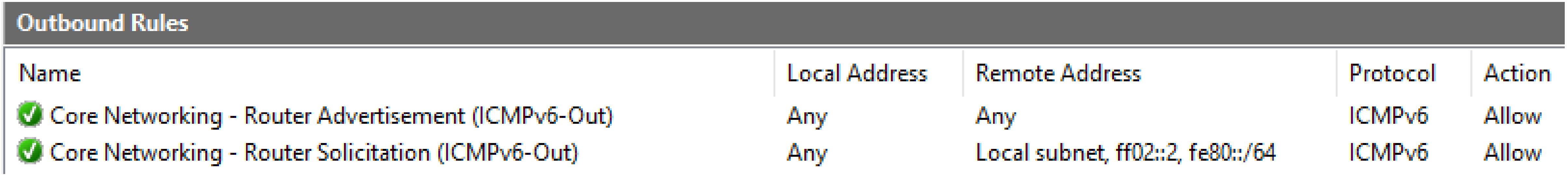
- Do we need Router solicitation and teredo? Are we a router?



```
Interface 11: WLAN

Scope        References  Last  Address
----------   ----------  ----  -------------------
0                     0  Yes   ff01::1
0                     0  Yes   ff02::1
0                     3  Yes   ff02::c
0                     2  Yes   ff02::fb
0                     1  Yes   ff02::1:3
0                     1  Yes   ff02::1:ff42:c32
0                     1  Yes   ff02::1:ff46:fcff
0                     2  Yes   ff02::1:ff6e:13f9
```

IPv6 outbound

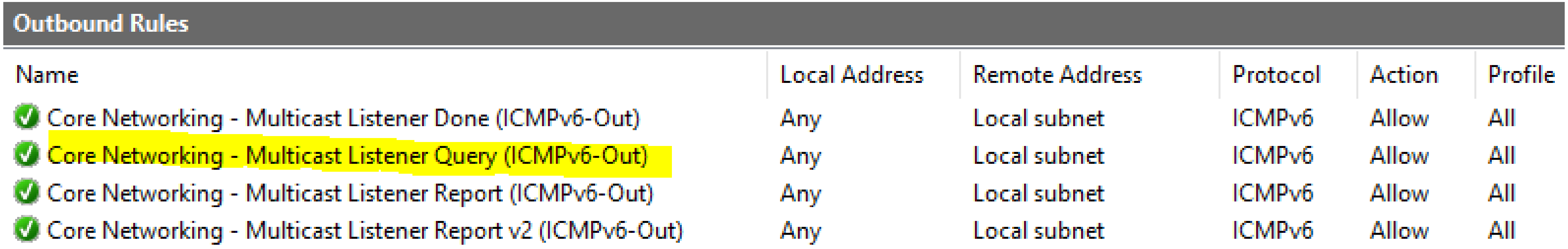


Outbound Rules

Name	Local Address	Remote Address	Protocol	Action
✓ Core Networking - Router Advertisement (ICMPv6-Out)	Any	Any	ICMPv6	Allow
✓ Core Networking - Router Solicitation (ICMPv6-Out)	Any	Local subnet, ff02::2, fe80::/64	ICMPv6	Allow

- Outgoing Router Advertisements are allowed
- We need Router Advertisement Guard on Switch
- This might be used for „Internet Connection Sharing“
  - Does anyone still use it?

ICMPv6 Multicast

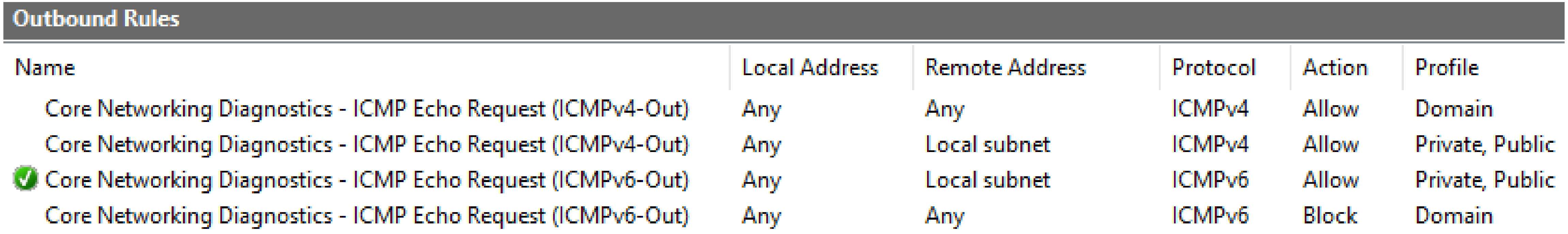


Outbound Rules

Name	Local Address	Remote Address	Protocol	Action	Profile
✓ Core Networking - Multicast Listener Done (ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	All
✓ Core Networking - Multicast Listener Query (ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	All
✓ Core Networking - Multicast Listener Report (ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	All
✓ Core Networking - Multicast Listener Report v2 (ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	All

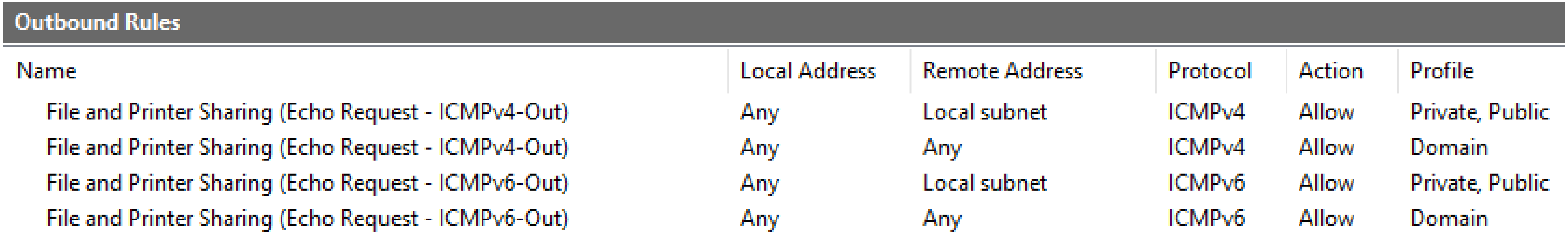
- Multicast Listener Query is send by routers
- Again, connection sharing?

ICMPv6 Ping



Outbound Rules

Name	Local Address	Remote Address	Protocol	Action	Profile
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-Out)	Any	Any	ICMPv4	Allow	Domain
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-Out)	Any	Local subnet	ICMPv4	Allow	Private, Public
✓ Core Networking Diagnostics - ICMP Echo Request (ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	Private, Public
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-Out)	Any	Any	ICMPv6	Block	Domain



Outbound Rules

Name	Local Address	Remote Address	Protocol	Action	Profile
File and Printer Sharing (Echo Request - ICMPv4-Out)	Any	Local subnet	ICMPv4	Allow	Private, Public
File and Printer Sharing (Echo Request - ICMPv4-Out)	Any	Any	ICMPv4	Allow	Domain
File and Printer Sharing (Echo Request - ICMPv6-Out)	Any	Local subnet	ICMPv6	Allow	Private, Public
File and Printer Sharing (Echo Request - ICMPv6-Out)	Any	Any	ICMPv6	Allow	Domain

- ICMP echo has two rulesets
- Be careful

Conclusion

- The Windows firewall is a host firewall
- The firewall is generally very open
- Used „at home“ and in the enterprise
- The firewall is ready for the PC to work as a router (Connection sharing)
- It is application oriented, not network oriented
- This firewall should be part of your **Cybersecurity** strategy