

# Advanced Configuration

---



**Richard Hicks**

Richard M. Hicks Consulting, Inc.

@richardhicks    [www.richardhicks.com](http://www.richardhicks.com)



# Overview



## Advanced Configuration

### Overview

- Name resolution
- Proxy server configuration
- Zero-trust Network Access (ZTNA)



# Name Resolution

---





## VPN client DNS server(s)

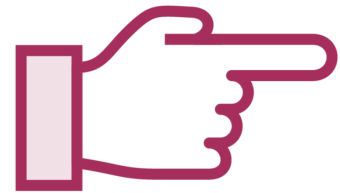
- DNS server(s) assigned to VPN server

## Recommended configuration

### Doesn't work when...

- VPN server does not use Active Directory DNS servers
- Perimeter/DMZ
- Non-domain joined

# Name Resolution Policy Table (NRPT)



**Policy-based name resolution request routing**



**Optional Configuration**



**Domain namespace or individual hosts**



**Proxy server supported (works only with Internet Explorer)**



NRPT is NOT supported with  
the device tunnel



# Demo



## Enable the Name Resolution Policy Table



# Name Resolution Policy Table in XML

```
<DomainNameInformation>  
  <DomainName>.corp.example.net</DomainName>  
  <DnsServers>10.21.12.200,10.21.12.201</DnsServers>  
</DomainNameInformation>
```





# Proxy Servers

---

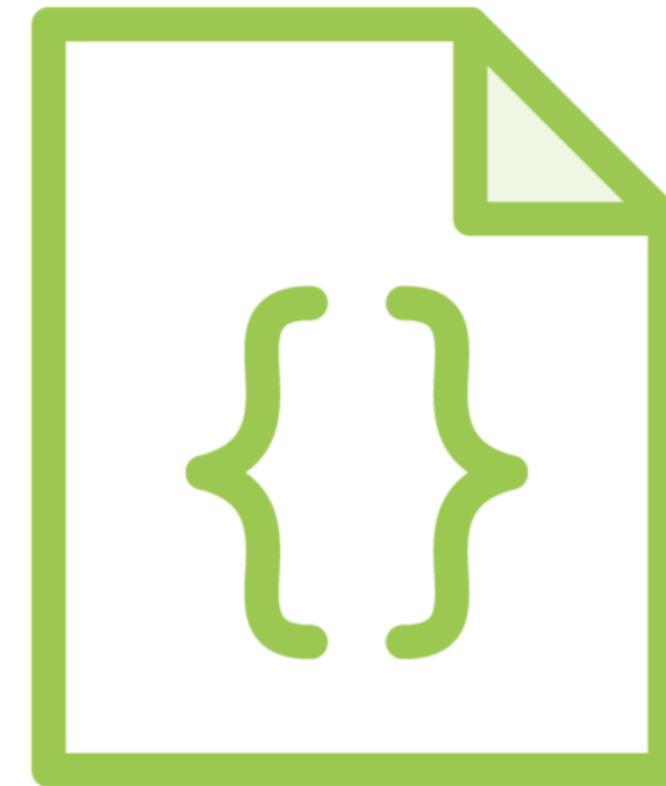


# Proxy Server Configuration



## Explicit

Proxy server hostname defined in configuration directly



## Auto Configured

Proxy server settings retrieved from Proxy Auto Configuration (PAC) file



Proxy settings only used on  
Force Tunnel connections



# Demo



## Configure VPN proxy settings



# Proxy Server Configuration - Explicit

```
<Proxy>  
  <Manual>  
    <Server>proxy.corp.example.net:8080</Server>  
  </Manual>  
</Proxy>
```



# Proxy Server Configuration - Autoconfigure

```
<Proxy>  
    <AutoConfiguURL>http://proxy.corp.example.net:8080/proxy.pac</AutoConfiguURL>  
</Proxy>
```



# Zero Trust Network Access

---



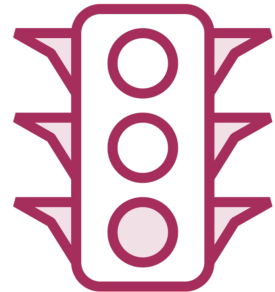
# Zero Trust Network Access

Zero trust network access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications.





# Zero Trust with Always On VPN



**Traffic filters**



**Source/destination IP address, protocol, source/destination port**



**Application filters**



**Executable, package family name, SYSTEM**



Traffic filters do NOT work with  
IPv6



# Zero Trust Considerations

## Advantages

- Limited network access
- Reduced attack surface
- Endpoint enforcement
- Easy to configure basic policies

## Disadvantages

- Increased complexity
- Difficult to manage and support
- Fixed policies
- Granular control requires XML



# Demo



## Configure Zero Trust network access



# Traffic Filter – RDP to Internal Subnet

```
<TrafficFilter>  
  <Protocol>6</Protocol>  
  <RemotePortRanges>3389</RemotePortRanges>  
  <RemoteAddressRanges>172.16.0.0/16</RemoteAddressRanges>  
</TrafficFilter>
```



# Traffic Filter – RDP for Application

```
<TrafficFilter>
  <App>
    <Id>C:\Windows\System32\mstsc.exe</Id>
  </App>
  <Protocol>6</Protocol>
  <RemotePortRanges>3389</RemotePortRanges>
  <RemoteAddressRanges>172.16.0.0/16</RemoteAddressRanges>
</TrafficFilter>
```



# Traffic Filter – RDP for Store App

```
<TrafficFilter>  
  <App>  
    <Id>Microsoft.RemoteDesktop_8wekyb3d8bbwe</Id>  
  </App>  
  <Protocol>6</Protocol>  
  <RemotePortRanges>3389</RemotePortRanges>  
  <RemoteAddressRanges>172.16.0.0/16</RemoteAddressRanges>  
</TrafficFilter>
```



# Summary



## Advanced Configuration

### Summary

- NRPT configuration
- Proxy server settings
- Application and traffic filtering





Up Next:  
Always On VPN in Azure

---

