



Segment Deployment Guide

Version: 5.2 January 2024

Proprietary notice: This document and the information contained in it are proprietary and confidential to Zero Networks LTD. No person is allowed to copy, print, reproduce or publish any part of it nor disclose its contents to others, not make any use of it, nor allow or assist others to make any use of it, unless by prior express written authorization of Zero Networks LTD. And then only to the extent authorized. Finders of this document are to destroy this copy and report its finding to office@zeronetworks.com © 2024 by Zero Networks LTD.





Table of Contents

1.	In	troduction	2
2.	Pr	Prerequisites	
2	.1.	Segment Server sizing	3
2	.2.	Network access requirements	4
	2.2	1.1 External network access requirements	4
	2.2	2.2 Internal network access requirements	5
2	.3.	Create a list of hosts to include for a PoC	6
2	.4.	Files and processes to exclude from security controls such as EDR	7
3.	De	ployment procedure	8
3	.1.	Create a Windows virtual machine	8
3	.2.	Active Directory requirements	8
3	.3.	Networking configuration	8
3	.4.	Provide details for first admin bootstrap user	8
3	.5.	Download Zero Networks Segment Server deployment package	9
3	.6.	Run setup	10
Ap	pen	dix A: Recommended GPO hardening	16
Ap	pen	dix B: AD Group Hardening	17





1. Introduction

This document describes the prerequisites and the procedure of deploying Zero Networks Segment.

Zero Networks is a revolutionary network attack prevention solution that automatically learns how your devices normally communicate and ensures network access is available only when needed – blocking all other connections, including malicious attempts to enumerate and traverse your network. By giving network access only to the devices that need it and only when they need it, Zero Networks prevents network discovery and lateral movement.

To ensure unusual but legitimate connections are not affected, Zero Network provides a bypass mechanism through a multi-factor (MFA) authentication wall on your users' mobile phones.

Zero Networks protects against both commodity threats and advanced attacks by regulating network connections, leaving threats with near zero network visibility and access. Because threats are contained, your security team saves cycles originally used to address alerts and hunt for undetected threat activity.

Our patent-pending technologies automatically learn and adapt to your network – you won't need to deal with complex rules to stay protected. There are no agents to deploy and update, or client apps that can impact end-user experiences.





2. Prerequisites

Zero Networks is a cloud network security solution and in order to operate it requires a component deployed in your network called: Segment Server.

The Segment Server machine that is installed from a deployment package that you can download from your Admin Portal.

These are the prerequisites for creating a new deployment:

2.1.	Segment Server sizing
------	-----------------------

Number of machines*	CPU (cores)	Memory (GB)	HD storage (GB)	Network adapter**
1,000	2	4	100	1 GB bridged
2,000	4	8	100	1 GB bridged
5,000	8	16	100	1 GB bridged
10,000	16	16	100	1 GB bridged

* This is the number of machines that one Segment Server is protecting

** The network adapter should be bridged and NOT in a NAT configuration





2.2. Network access requirements

The following diagram and table describe the minimum ports that must be opened for the Segment Server to work properly:



Customer's environment

2.2.1 External network access requirements

Protocol	Transport	Port	From	То	Direction	Description
HTTPS	ТСР	443	Segment Server	*.zeronetworks.com (34.74.201.149) ¹	Outbound	Used by the Segment Server to retrieve data and commands to/from the Zero Networks Segment cloud
HTTPS	ТСР	443	Segment Server	monitor.zeronetworks.co m (35.201.109.138) ¹	Outbound	Used by the Segment Server to send health and performance metrics to the Zero Networks Segment cloud





2.2.2 Internal network access requirements

Protocol	Transport	Port	From	То	Direction	Description
WinRM	ТСР	5985	Segment Server	All Windows assets	Outbound	Used to retrieve information and control the firewall of Windows assets
SSH	ТСР	22	Segment Server	All Linux assets	Outbound	Used to retrieve information and control the firewall of Linux assets
HTTPS	TCP and UDP	443	All assets	Segment Server	Inbound	Used to trigger JIT (MFA)

LDAP	ТСР	389	Segment Server	Domain controllers	Outbound	
LDAPS	ТСР	636	Segment Server	Domain controllers	Outbound	Used to retrieve information from
Global Catalog LDAP	ТСР	3268 and 3269	Segment Server	Domain controllers	Outbound	Active Directory
Kerberos	TCP and UDP	88	Segment Server	Domain controllers	Outbound	
NTLM	ТСР	135 and 445	Segment Server	Domain controllers	Outbound	Used for authentication
DNS	TCP and UDP	53	Segment Server	DNS Servers	Outbound	Used to retrieve IP and FQDN information from DNS

Note¹: following is the complete list of all Zero Networks domains required to be accessible:

- portal.zeronetworks.com
- access.zeronetworks.com
- 2fa.zeronetworks.com
- cloud-prod-v2.zeronetworks.com
- register-prod.zeronetworks.com
- register-cloud-connector.zeronetworks.com





- cloud-connector.zeronetworks.com
- jamf-connector.zeronetworks.com
- connect-backend.zeronetworks.com
- connect-auth.zeronetworks.com
- connect.zeronetworks.com
- download.zeronetworks.com
- monitor.zeronetworks.com

nnectivityTest.ps1

Please run the following PowerShell script to test network connectivity to the hostnames and required ports: https://github.com/zeronetworks/Community/blob/master/Segment/Troubleshooting/ZNCo

Note²: all communications between the Segment Server and the cloud service should bypass the proxy. In case you have proxy in your environment, see <u>Appendix B: Proxy configuration</u> for more details.

Note³: Given that Zero Networks implemented mutual authentication TLS (mTLS) to ensure security and privacy of communications with its Cloud services, some firewalls, IPS or IDPS systems might break HTTP/2 and/or gRPC communications. During setup or after installation if you see errors like "authentication handshake failed: context deadline exceeded" this is an indicator one of these systems is causing an issue. It is therefore advised to allowlist traffic towards Zero Networks Cloud services, bypassing any possible traffic inspection/interception.

2.3. Create a list of hosts to include for a PoC

If you're deploying as part of a Proof of Concept (PoC), it's good to know we can monitor & protect a selection of assets. To speed up the PoC deployment, please prepare a list of hostnames which you would like to add to the PoC. We recommend anything between 20 and 50 hosts, ideally a mix of client and server assets.

Later during the deployment, you will need to add these hostnames to a group called "ZeroNetworksMonitoredAssets" in AD.



2.4. Files and processes to exclude from security controls such as EDR

It's recommended to exclude the following from your EDR to avoid false positive alerts & installation failures:

- Directory: on the trust server exclude file path "C:\Program Files\Zero Networks\" and directories underneath, from file scanning.
- Process: on the assets part of the PoC a WSMPROVHOST.EXE process will be running under the context of the service account (the service account is defined during trust server setup).

In recent engagements we have seen Cisco AMP and Bitdefender remove critical files, we recommend adding exclusions to the locations/process mentioned above to prevent issues.





3. Deployment procedure

3.1. Create a Windows virtual machine

In your virtual infrastructure (Hyper-V / VMWare) create a Windows VM with the following resources:

- Operating system:
 - Windows Server 2019 (minimum build 17763) or
 - Windows Server 2022 (minimum build 20348)
- o CPU: 4 cores
- o RAM: 8 GB
- Hard disk: 100 GB
- Network: 1GB bridged network adapter (not NATed)

Note:

- o Standard Windows installation without any special windows features
- Operating system language should be English
- The virtual machine should be domain joined
- The virtual machine should have a static IP address

3.2. Active Directory requirements

It's recommended to join the Segment server to the forest root. Zero Networks Segment supports adding additional child domains in the same forest or add additional forests and child domains.

3.3. Networking configuration

In your enterprise network firewall, open the required list of ports for the Segment Server to work properly (see Prerequisites: Ports open in network firewall).

In addition, in case you have a network proxy, see <u>Appendix B: Proxy configuration</u> for more details.

3.4. Provide details for first admin bootstrap user

A bootstrap user is required for the initial login to the Admin Portal prior to the integration with your environment (post initial setup and integration you will use users from your identity provider).

Note: the user should have access to his email to receive the verification code





Please send your Zero Networks point of contact the following details:

- Full name
- o Email address

3.5. Download Zero Networks Segment Server deployment package

• Browse to <u>portal.zeronetworks.com</u> and login with your email \rightarrow click **sign in**

Please sign in to your account
Work email
polina@zeronetworks.com
Sign in
OR
Sign in with Microsoft
Sign in with Duo
Sign in with Okta
Having trouble signing in? <u>Contact support</u>





• Authenticate with the code that was sent to your email \rightarrow click **verify**

	A verification code has been sent to polina@zeronetworks.com
/erifica	tion code
719	282
Sen	id a new verification code via <u>phone</u> or <u>email</u>
	Verity
	OR
	Sign in with Microsoft
	Sign in with Duo
	Sign in with Okta

• Navigate to Settings \rightarrow Segment \rightarrow Segment servers \rightarrow click Download

Settings	
System	Segment servers
Roles	Deumlaad
Mail notifications	Download
Portal security	
Internal subnets	Name
Segment	
Segment servers	
Cloud connector	

3.6. Run setup

- Copy the downloaded deployment package to the C drive on the Segment Server
- Run trust-setup.exe
 - **Note:** the user should be a domain admin



• Click "Next" to start the setup

2 C:\Users\Administrator\Desktop\windows-trust-3.0.0.42\trust-setup.exe				
Welcome to Zero Networks Trust Setup! Version 3.0.0.42				
Next				

• Authenticate with the first admin bootstrap user (this is the user you used to login to the admin portal to download the setup)

C:\Users\Administrator\Desktop\windows-trust-3.0.0.42\trust-setup.exe -	\times
MFA validation	
Email polina@zeronetworks.com	
Next	



• Enter the verification code

2 C:\Users\Administrator\Desktop\windows-trust-3.0.0.42\trust-setup.exe				
Verification code sent				
Verification code 305470				
Back Resend Code Next				

• Fill in the deployment parameters

Z Administrator: C:\Users\yossitest\Desktop\windows-trust-3.0.10.5\trust-setup.exe			×
Deployment	Parameters		
Domain	lab11.zn.com		
Domain Controller FQDN	lab11-dc8r2.lab11.zn.com		
The Zero Networks remote management user (SAMAccountName)	znremotemanagement		
Password for the Zero Networks remote management user	******		
Create AD Prerequisites	×		
Zero Networks' AD Prerequisites user and groups OU path	OU=ZeroNetworks,DC=lab11,DC=zn,DC=com		
Next			

Note: The "Create AD prerequisites" option will create the following in Active Directory:

- 1 user ("ZNRemoteManagment") this user will be granted permissions to perform remote firewall operations through WinRM
- o 3 groups
 - "ZeroNetworksMonitoredAssets" contains all computers to be monitored by Zero Networks – manually managed by the customer





- "ZeroNetworksProtectedAssets" contains all computers protected by Zero Networks – automatically managed by Zero Networks when an asset moves to protection mode
- "ZNRemoteManagementGroup" contains the "ZNRemoteManagment" user, used in various GPO setting for WinRM permissions and hardening
- o 2 GPOs
 - "ZeroNetworksMonitor" enables the Segment Server to remotely monitor the assets (by default will be applied to the Authenticated Users and

"ZeroNetworksMonitoredAssets"	group)
-------------------------------	--------

📓 Group Policy Management	ZeroNetworksMonitor		
 A Forest: zerodemo.local Company Domains 	Scope Details Settings Delegation		
 ✓ A Contains ✓ A Contains ✓ Perodemolocal ✓ Default Domain Policy ✓ ZeroNetworksMonitor ✓ Domain Controllers ✓ Domain Controllers ✓ ZeroNetworks ✓ Group Policy Objects ✓ WMI Filters ✓ Starter GPOs ✓ Sites ✓ Group Policy Modeling ✓ Group Policy Results 	Links Display links in this location: zr The following sites, domains, and OUs an Location	erodemo.local e linked to this GPO: Enforced Yes	Link Enabled Path Yes zerodemo.local
Croup Poicy Kesuits	Security Filtering The settings in this GPO can only apply to Name & Authenticated Users & ZeroNetworksMonitoredAssets (ZER	the following groups, usen	s, and computers: nitoredAssets)

 "ZeroNetworksProtect" – turns on the host-based firewall of assets in the assigned group and hardens important firewall configuration, will only be

applied to assets in the "ZeroNetworksProtectedAssets"

📓 Group Policy Management	ZeroNetworksProtect			
 A Forest: zerodemo.local 	Scope Details Settings Dele	egation		
🗸 📑 Domains		gaton		
✓ jii zerodemo.local	Links			
🔊 Default Domain Policy	Display links in this location:	zerodemo.local		
漏 ZeroNetworksMonitor	The following sites, domains, and	OUs are linked to this GPO:		
📷 ZeroNetworksProtect				
Domain Controllers	Location	Enforce	d Link Enabled	Path
> 🧊 ZerodemoUsers	zerodemo.local	Yes	Yes	zerodemo.local
> 🧊 ZeroNetworks				
> 📑 Group Policy Objects				
> 📑 WMI Filters				
> 🧊 Starter GPOs				
> 📑 Sites				
🔐 Group Policy Modeling				
Group Policy Results				
	Security Filtering			
	The settings in this GPO can only	apply to the following groups	users, and computers:	
	Name			
	R ZeroNetworksProtectedAss	ats (ZERODEMO)/ZeroNetwork	ProtectedAssets)	
			a, 10100100, 100010)	

© 2024 by Zero Networks LTD. All Rights Reserved.

support@srccybersolutions.com





• Wait for all the tests to pass successfully

Z Administrator: C:\windows-trust-3.0.11.0\t	rust-setup.exe		×
Minimum hardware requirements OS requirements Get network info Check DNS resolution Cloud connectivity Applying GPO automation Domain Controller connectivity			
Back Next			

• Wait for the deployment to finish successfully

Z Administrator: C:\Users\Administrator\Desktop\windows-trust-3.0.0.42\trust-setup.exe			×
	Deploying		
Installing dependencies Configuring system Installing certificates Init services Registering Deployment Initializing environmment files Initializing keys Setting up monitoring Starting services			
Next			





• Click "Finish" to exit setup

2 Administrator: C:\Users\Administrator\Desktop\windows-trust-3.0.0.42\trust-setup.exe	-	\times
You have successfully installed LAB16-TRUST as a new trust server		
Finish		





Appendix A: Recommended GPO hardening

For security reasons, it's recommended to harden the following settings in the

ZeroNetworksMonitor GPO in case they are not already hardened by another GPO and don't

conflict with your needs:

Setting	Setting Path	Setting Value
Safeguard the Zero Networks User and Groups	Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally	ZNRemoteManagementGroup
	Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services	ZNRemoteManagementGroup
WinRM Configuration	Computer Configuration\Policies\Administra tive Templates: Policy definitions (ADMX files) retrieved from the local machine\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic Authentication	Disabled
	Computer Configuration\Policies\Administra tive Templates: Policy definitions (ADMX files) retrieved from the local machine\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic	Disabled





Appendix B: AD Group Hardening

Only the Zero Networks service account should add machines to the Zero Networks Protected Assets AD group. Moving systems into this group outside of the portal will cause systems to block all Inbound and Outbound connections resulting in dropped network connections and unwanted behavior. To prevent this unwanted behavior, it is recommended to remove permissions from all other groups in AD.

Permissions required:

- SYSTEM Full Control
- ZNRemoteManagement Group Full Control
- Authenticate Users Read

)wner:	Domain Admins (PARTNERSZ	N\Domain Admins)	Change		
Permissions	Auditing Effective Ac	cess			
or additiona	l information, double-click a perr	nission entry. To mod	dify a permission entry, select	t the entry and click Edit (if availab	ole).
ermission e	ntries:			-	
Туре	Principal	Access	Inherited from	Applies to	
Illow	Authenticated Users	Send to	None	This object only	
🚨 Allow	ZNRemoteManagementGrou	Full control	None	This object only	
👢 Allow	SELF	Special	None	This object only	
👢 Allow	Authenticated Users	Special	None	This object only	
🚨 Allow	SYSTEM	Full control	None	This object only	
Add	Remove View			Restore defa	ulte
Auu	Remove view	0.0.0		Restore della	unts





Appendix B: Proxy configuration

To make sure your Segment Server is routing properly through the proxy, you should configure the

environment variables required for the proxy:

```
HTTP_PROXY = http://<proxy_server_ip>:<port>
HTTPS_PROXY = https://<proxy_server_ip>:<port>
NO_PROXY = localhost, 127.0.0.1
ZN_SKIP_CONN_TEST = true
```

Note: in some cases, a reboot of the server is required after adding the environment variables.

To verify that the Segment Server is routing outbound traffic via the configured proxy, find the

process ID of Zero Networks Remote service using the following command:

Get-Ser	rvice ? {\$Name -ma	tch "^zn"}
PS C:∖Us	ers\administrator.T	<pre>EACHJING> Get-Service ? {\$Name -match "^zn"}</pre>
Status	Name	DisplayName
Running	znad	Zero Networks ActiveDirectoryManager
Running	znadmin	Zero Networks Admin
Running	znansiblemanager	Zero Networks AnsibleManager
Running	znconfig	Zero Networks Config
lunning	znwinrm	Zero Networks RemoteManager

Look at all outbound connections from the Segment Server and verify they are routing through the proxy by referencing the process ID from the previous command.

netstat -ano | findstr <processID>

PS C:\Us	ers\jing> tasklist [.]	f <mark>indstr</mark> Remote		
ZeroNetw	orks.Trust.Remote	7484 Services	0	126,488 K
ZeroNetw	orks.Trust.Remote	7396 Services	0	27,524 K
PS C:∖Us	ers\jing> <mark>netstat</mark> -a	no findstr 7484		
TCP	10.60.0.189:50171	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50172	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50173		ESTABLISHED	7484
TCP	10.60.0.189:50174	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50175	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50176	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50177	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50178	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50179	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50180	10.60.0.203:3128	ESTABLISHED	7484
TCP	10.60.0.189:50183	10.60.0.203:3128	ESTABLISHED	7484

© 2024 by Zero Networks LTD. All Rights Reserved.

support@srccybersolutions.com