Tempered – CyberArk Integration Guide

CyberArk's Industry-Leading Privileged Access Management Solutions Leverage Tempered's Airwall Solution to Access Traditionally Air-Gapped Systems

Table of Contents

Introduction

CyberArk provides industry-leading Privileged Access Management solutions allowing many industries to reduce their cybersecurity risks by addressing the many aspects of privileged access security.

Tempered’s Airwall solution is the Zero-Trust, Software-Defined Perimeter for all your critical assets. Tempered enables customers to create encrypted, perfect-forward secrecy, tunneled connections into previously air-gapped environments for secure access, all without turning over the keys to a Software-as-a-Service (SaaS) vendor.

Combined, Tempered’s Airwall allows CyberArk’s products to securely reach into hyper-secure environments like Operational Technology (OT) and Industrial Control Systems (ICS) to perform the necessary access or password management.

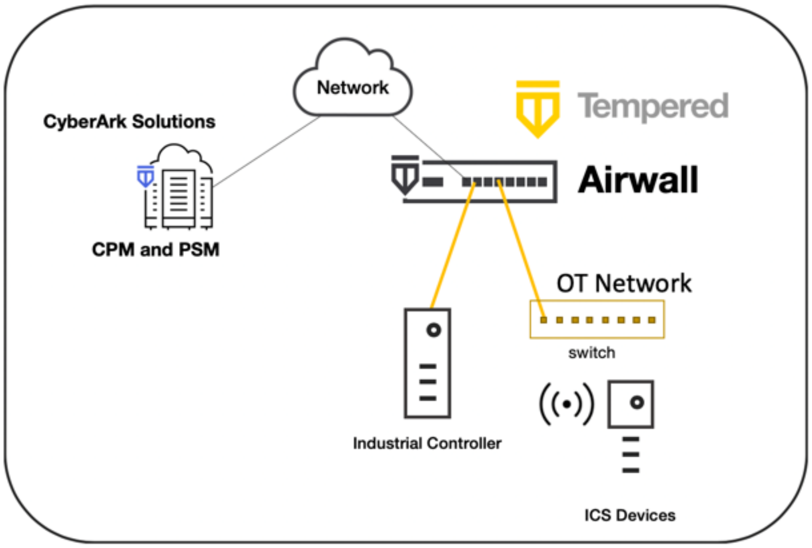
Airwall™ makes ‘things’ on a network invisible and protects against cyber-attacks. Airwall is a comprehensive solution that is exceptionally effective at protecting critical physical infrastructure, while still allowing secure remote access. Airwall Solutions extend to cloud, virtual, and physical environments. Secure every endpoint in your network, from local data center to global infrastructure. Provide global connectivity and mobility for your entire infrastructure, wherever the systems are and for whatever they need to reach, securely.

Overview

For many managed devices, the server, IOT device or network element needs to be on the general network to perform its function – like Active Directory or a DNS Server. But for an increasingly larger number of devices, they need to be micro-segmented to reduce cybersecurity threats and exposure from lateral movement. Traditionally there were a whole class of devices that were air-gapped from the general network. OT and ICS devices are typical examples of devices that were often on a separate network that had no connectivity to the Internet or general network.

Privileged access security is a good example of a solution that provides a significant benefit to an organization but requires that a system have both access to users and access to hyper-secure, critical infrastructure devices. In other words, this use case can be the first reason a company considers moving devices out from the air gap. Rather than setting up systems that bridge multiple VLANs and require very complex and expensive designs using internal firewalls, Airwall allows simple, secure access into the virtually air-gapped environment.

CyberArk's products - including Privileged Session Manager (PSM) and Centralized Policy Manager (CPM) - require access to these hyper-secure environments to be able to perform their functions on these systems or devices. In addition, if CyberArk's Alero users connecting to Vault need access via Core Privileged Access Security – Tempered can provide the gateway into these OT or ICS devices.



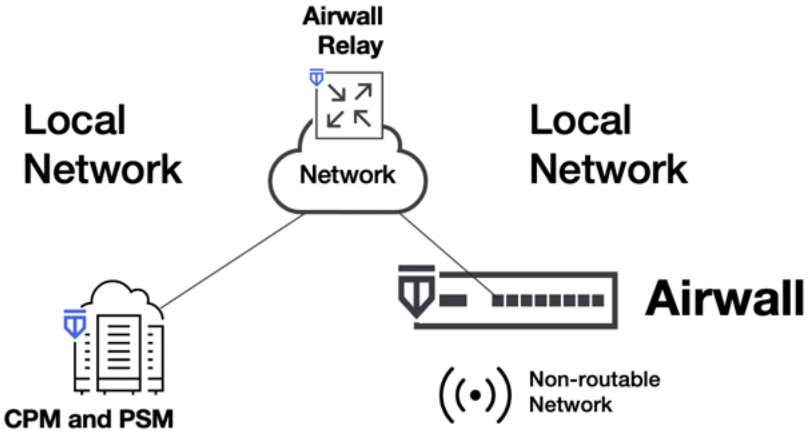
This integration guide will describe the implementation details required to design and implement a Tempered/CyberArk solution for this use case.

Solution Flexibility

In today's networked world, the location of CyberArk's servers and the devices they need to access can come in many different combinations. Tempered's Airwall solution includes a component called Airwall Relay that allows encrypted connectivity between any non-routable networks. This could be two networks within a manufacturing facility that do not have connectivity for security reasons, or they could be diverse networks spanning the globe. The following combinations are supported with the integration described in this guide.

Local Network to Local Network

In a traditional networking environment consisting of a single facility, devices that were traditionally air-gapped may continue to live on a non-routable network from the perspective of CyberArk PSM/CPM. In this design, an Airwall would be added as a secure gateway, which can be physical or virtual, and the Airwall Server would be installed on CyberArk. The Airwall could either have a leg into the Local Network that was reachable by CyberArk or an Airwall Relay could be deployed such that CyberArk and the Airwall could reach the Relay (outbound UDP 10500). One possible solution would be to install the Relay in the corporate DMZ that was reachable from each network. The industrial or OT devices are still only reachable from the CyberArk server, not any other hosts on the Local Network.

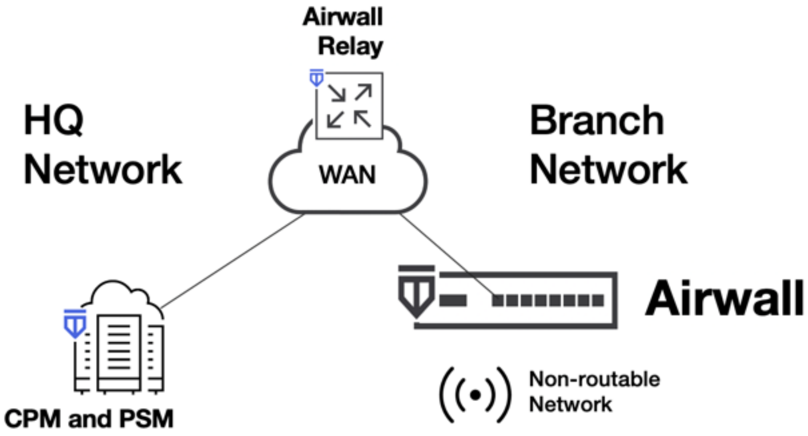


HQ Network to Branch Network

In a typical HQ to branch style network, there is often a WAN connecting the two locations, although in some cases this is just the Internet. Either scenario will work with this integrated solution as long as the Airwall Relay is deployed such that the CyberArk server and the Airwall have outbound network connectivity (UDP 10500) to the Relay.

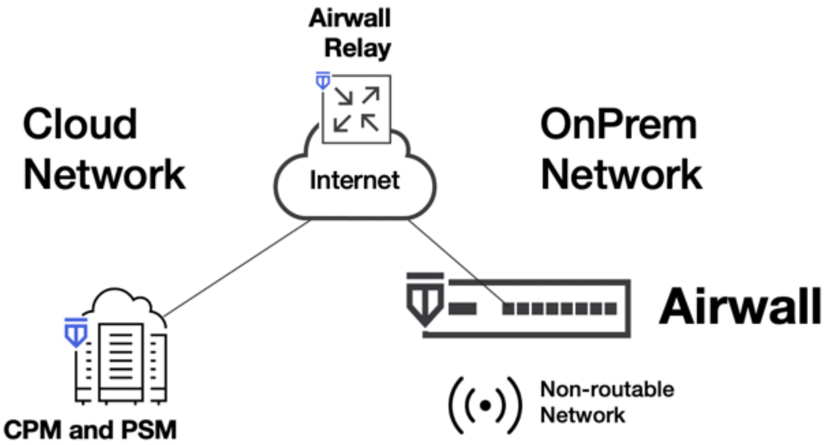
Any type of WAN transport is viable, showcasing the flexibility of the Airwall solution to provide "secure plumbing" between any two locations for any protocol. As a reminder, with all of Tempered's scenarios you maintain complete control over the solution elements avoiding having to hand over the keys of your network to a Software-as-a-Service Cloud provider.

When the CyberArk PSM or CPM needs to access a device, it will establish a Host Identity Protocol tunnel through the Relay on demand.



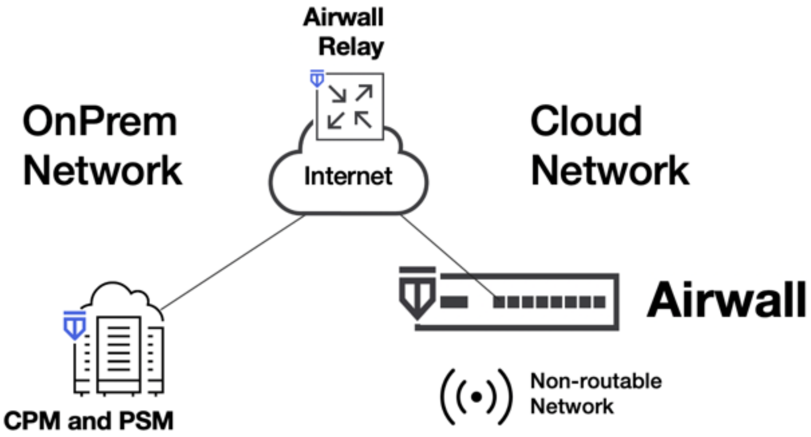
Cloud Network to OnPrem Network

In some scenarios you may choose to deploy CyberArk in the Cloud – Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform. In this case, the devices requiring hyper-secure security remain behind the Airwall Gateway. The Internet is now the transport for the CyberArk server to reach the Airwall Relay. In addition, the Airwall must have outbound connectivity to an Internet addressed Airwall Relay. No port forwards or inbound firewall changes are needed to allow CyberArk to communicate to the OnPrem network. CyberArk and the Airwall reach out to the Relay and determine if they have policy to communicate and establish an AES-256 encrypted tunnel. Data communication is never unencrypted in the Relay assuring you of the utmost security when using Internet transport.



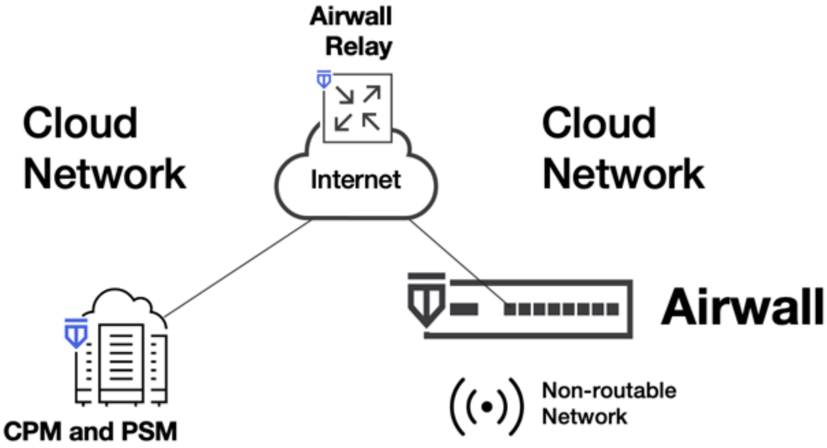
OnPrem Network to Cloud Network

Similarly, you may already have deployed CyberArk in your OnPrem network and now need to reach out to Cloud devices. Tempered's Airwall can be deployed as a virtual gateway in cloud environments. Using the Relay to provide network connectivity between these non-routable networks, PSM/CPM can now easily reach into cloud environments to perform its functions.



Cloud Network to Cloud Network

Finally, if both the CyberArk server and devices it needs to connect to are in Cloud virtual networks, Airwall can be deployed to provide secure, flexible plumbing into the cloud infrastructure. If you migrate to a different cloud environment or migrate from data center to cloud, the secure access would not change. With Tempered's Host Identity Protocol based security, the cryptographic ID follows the Airwall rather than being locked down to an IP-based location making it extremely flexible.


Airwall
Relay
Cloud
Network
Internet
Cloud
Network
Airwall
CPM and PSM
Non-routable
Network

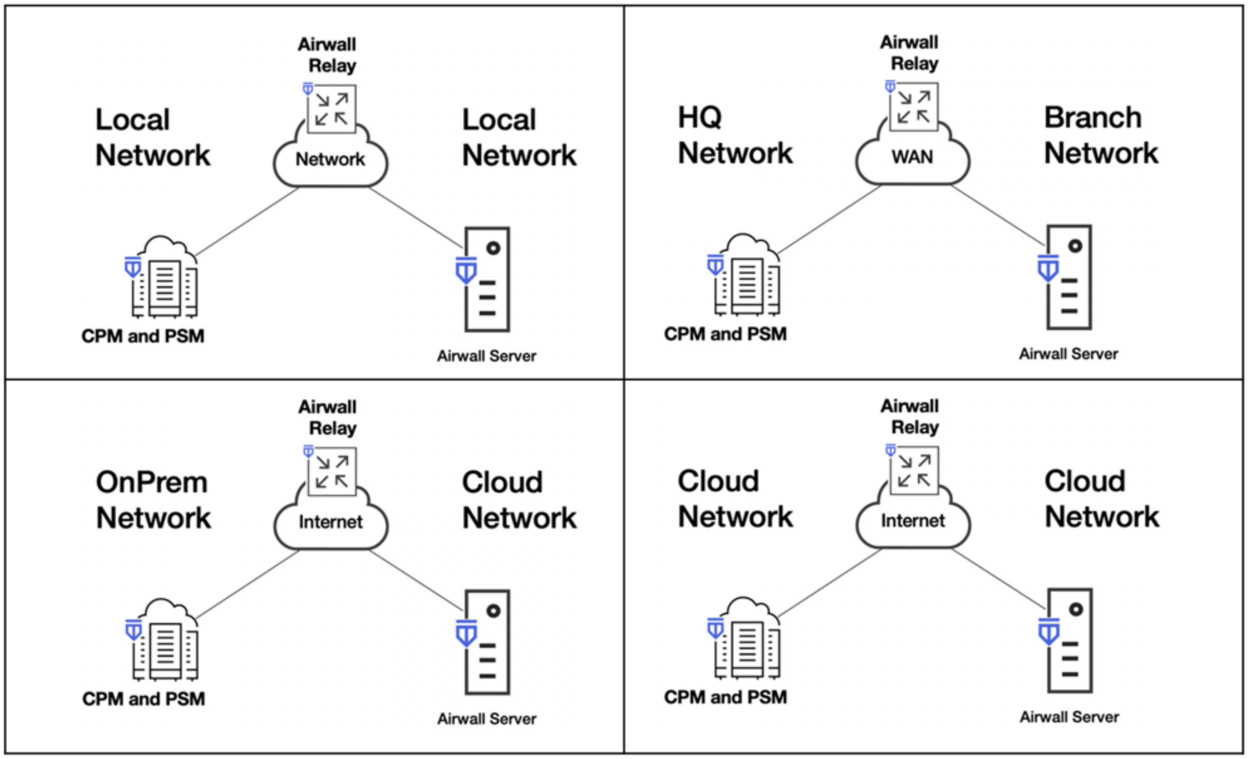
CyberArk Server to Protected Server

In addition to enabling CyberArk to access devices protected behind a physical or virtual Airwall Gateway, this integrated solution can also be deployed to allow CyberArk to access servers that are not networked or reachable from PSM/CPM. The Airwall Relay is providing the connectivity between the non-routable networks as long as each server can reach the Relay. This is common, especially in cloud environments. Tempered's Airwall Server is supported on Windows, MacOS and Linux.

In this design, the Airwall Server will be split-tunnel, allowing it to access the rest of its normal network, but CyberArk can reach it through a secure, encrypted tunnel via the Relay if necessary.

Airwall Server runs as an always on service such that all policy is controlled from a centralized component called the Conductor. No local configuration is required after the one-time install of the agent.

In the following diagram, Airwall Server is running on both the CyberArk server and the server it needs to reach.



Install Airwall Server on CyberArk PSM

The first step in setting up a CyberArk/Tempered combined solution is to install the Airwall Server agent on the CyberArk PSM or CPM server. The following prerequisites must be in place in order to take this first step:

Prerequisite	Description
Tempered Conductor	The Conductor is the central orchestration engine for all of the Tempered components. You must have a Conductor set up with available licensing for Airwall Server.
Tempered Airwall Gateway	In this example integration it is assumed that devices needing access (OT or ICS environment) are already protected and configured behind an Airwall Gateway.
Tempered Relay	If the CyberArk PSM does not have network reachability to the Airwall Gateway Underlay (encrypted) port, an Airwall Relay should be deployed to allow the non-routable networks to reach each other. This integration example will utilize an Airwall Relay.
CyberArk PSM - Admin Rights	You must have admin rights on the CyberArk PSM server so that they Airwall Server software can be installed which includes adding a TAP interface.

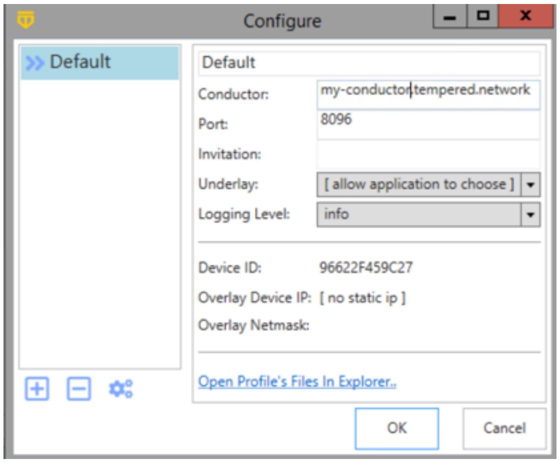
Follow these steps to configure the Airwall Server

1. **Download Software**

   Go to webhelp.tempered.io and download the Airwall Server software for your environment. Windows is being used in this example.

2. **Install the Airwall Server software on the PSM**

   During the installation you will be prompted to enter the URL of your Conductor:



Default

Conductor: my-conductor.tempered.network

Port: 8096

Invitation:

Underlay: [allow application to choose]

Logging Level: info

Device ID: 96622F459C27

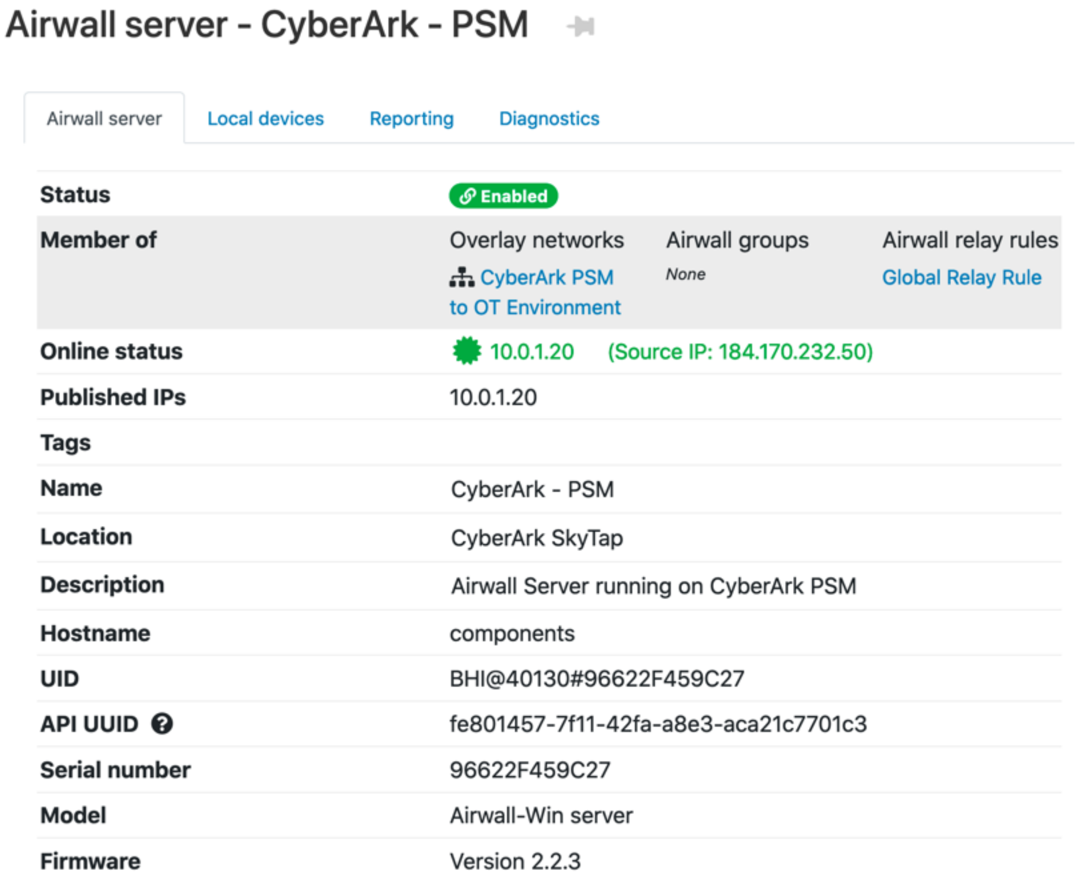
Overlay Device IP: [no static ip]

Overlay Netmask:

3. **Grant the provisioning request and manage the Airwall Server in the Conductor**

   This establishes the cryptographic identity that will be unique to this instance of an

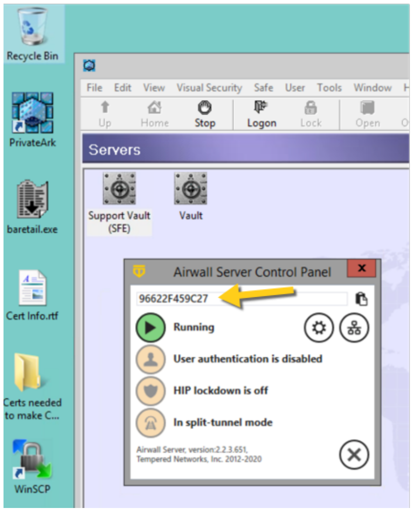
Airwall and allow it to establish HIP tunnels using its Host Identity Tag.



Airwall server - CyberArk - PSM

Status	Enabled
Member of	Overlay networks: CyberArk PSM to OT Environment Airwall groups: *None* Airwall relay rules: Global Relay Rule
Online status	10.0.1.20 (Source IP: 184.170.232.50)
Published IPs	10.0.1.20
Tags	
Name	CyberArk - PSM
Location	CyberArk SkyTap
Description	Airwall Server running on CyberArk PSM
Hostname	components
UID	BHI@40130#96622F459C27
API UUID ?	fe801457-7f11-42fa-a8e3-aca21c7701c3
Serial number	96622F459C27
Model	Airwall-Win server
Firmware	Version 2.2.3

Important: You will always want to verify the Device ID of the server before accepting the provisioning request to verify this is the server that should receive trust into the protected environment.



Recycle Bin
PrivateArk
baretail.exe
Cert Info.rtf
Certs needed to make C...
WinSCP
File Edit View Visual Security Safe User Tools Window
Up Home Stop Logon Lock Open
Servers
Support Vault (SFE)
Vault

Airwall Server Control Panel

96622F459C27

Running

User authentication is disabled

HIP lockdown is off

In split-tunnel mode

Airwall Server, version:2.2.3.651,
Tempered Networks, Inc. 2012-2020

Troubleshooting Airwall Server

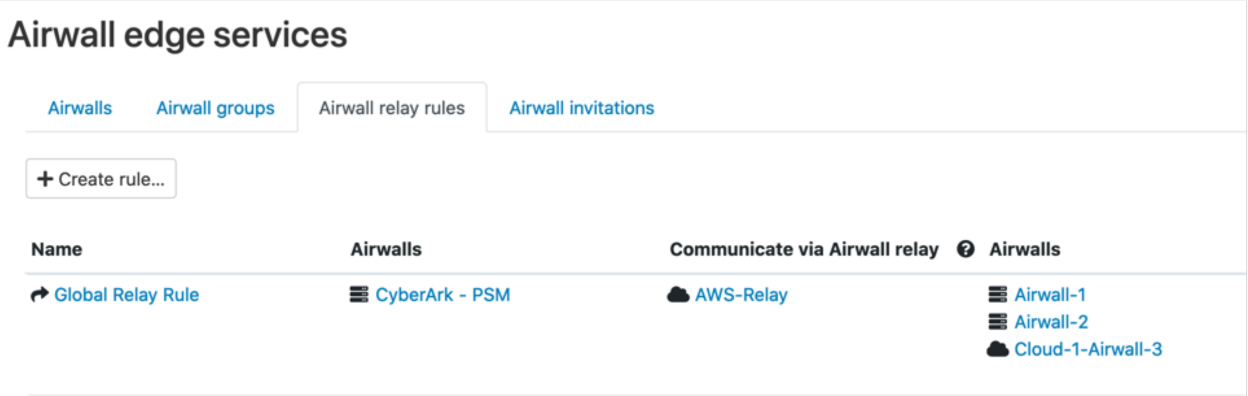
The CyberArk server where Airwall Server is installed must have connectivity to the Conductor using port TCP 8096. If the Airwall Server provisioning request does not show up in the Conductor verify that the Conductor is reachable (ping) and that TCP 8096 and TCP 443 are open to the Conductor.

Create Relay Rule and Overlay

There are two main items to set up in order to establish policy for the CyberArk PSM to talk to the protected OT devices. Establish an Airwall Relay rule if a relay is being used for connectivity and create an Overlay to establish trust between the particular IP hosts.

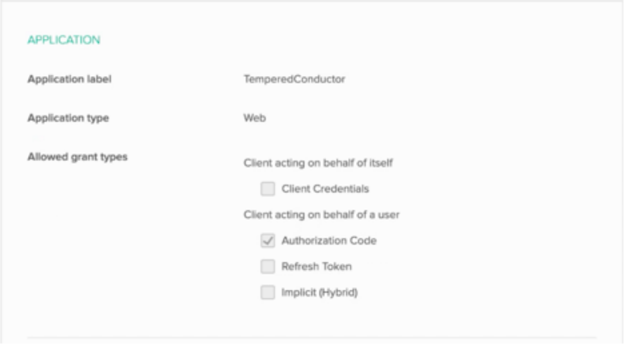
Add an Airwall Relay Rule

1. **In the Conductor, go to the Airwalls tab and verify that a relay rule exists (or add one) that allows the new Airwall Server to communicate via the Relay to the Airwall that is the Gateway for the protected devices. Here is an example:**



Airwall edge services

Name	Airwalls	Communicate via Airwall relay	Airwalls
Global Relay Rule	CyberArk - PSM	AWS-Relay	Airwall-1 Airwall-2 Cloud-1-Airwall-3



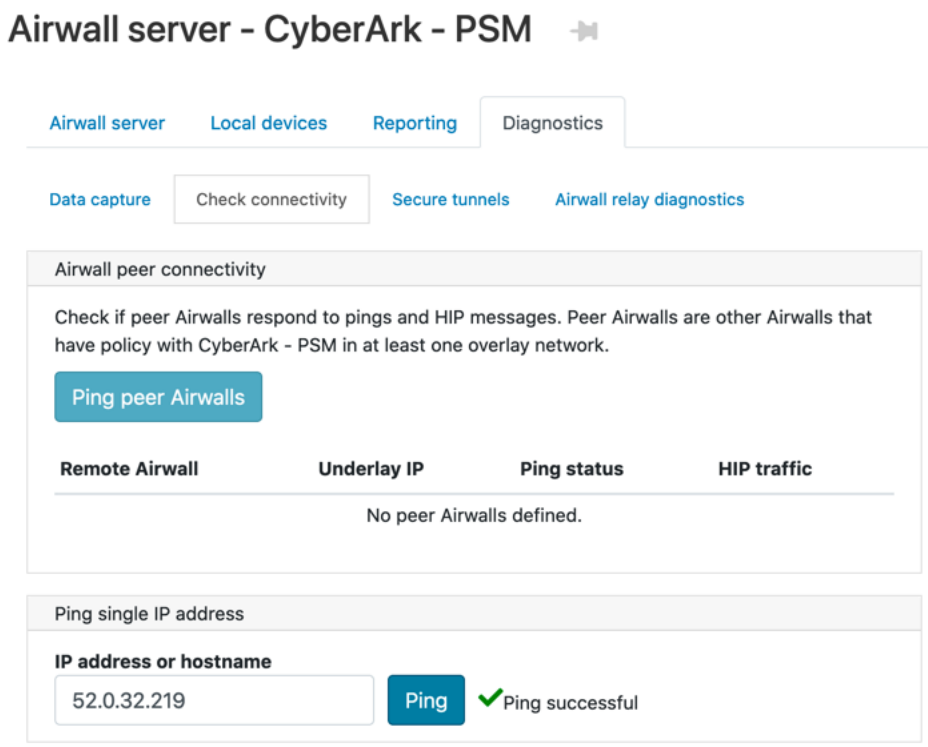
APPLICATION

Application label: TemperedConductor

Application type: Web

Allowed grant types:
Client acting on behalf of itself
□ Client Credentials
Client acting on behalf of a user
☑ Authorization Code
□ Refresh Token
□ Implicit (Hybrid)

2. Verify that the Airwall Server can reach the Airwall Relay using both ICMP and UDP 10500 – the port the Airwall Server will use to establish a tunnel through the relay. You can test this using the Conductor.



Airwall server - CyberArk - PSM

Airwall peer connectivity

Check if peer Airwalls respond to pings and HIP messages. Peer Airwalls are other Airwalls that have policy with CyberArk - PSM in at least one overlay network.

Remote Airwall	Underlay IP	Ping status	HIP traffic
No peer Airwalls defined.			

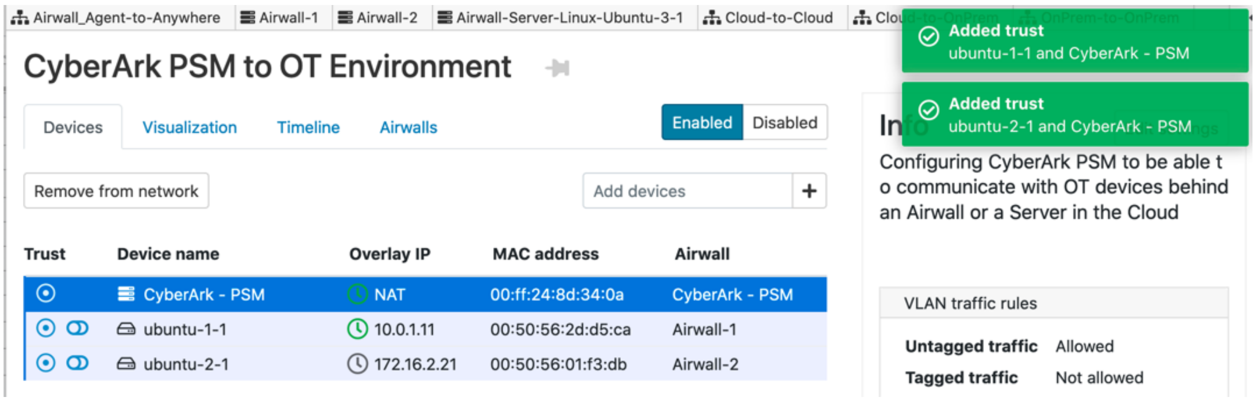
Ping single IP address

IP address or hostname: 52.0.32.219

✓ Ping successful

Create an Overlay

1. In the Conductor create an Overlay that includes both the CyberArk PSM and the devices it needs to reach (ubuntu-1-1 and ubuntu-2-2 in this example). Note that you do not need to configure which Airwall Gateway they are behind. Tempered's internal routing will automatically figure that out so that the Airwall Server on the PSM automatically knows which gateway to establish a tunnel with.



CyberArk PSM to OT Environment

Added trust
ubuntu-1-1 and CyberArk - PSM

Added trust
ubuntu-2-1 and CyberArk - PSM

Trust	Device name	Overlay IP	MAC address	Airwall
⊙	CyberArk - PSM	NAT	00:ff:24:8d:34:0a	CyberArk - PSM
⊙	ubuntu-1-1	10.0.1.11	00:50:56:2d:d5:ca	Airwall-1
⊙	ubuntu-2-1	172.16.2.21	00:50:56:01:f3:db	Airwall-2

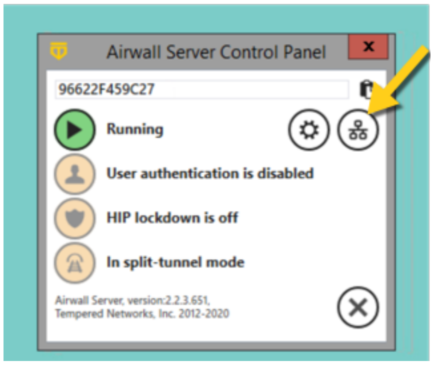
Info

Configuring CyberArk PSM to be able t o communicate with OT devices behind an Airwall or a Server in the Cloud

VLAN traffic rules

Untagged traffic	Allowed
Tagged traffic	Not allowed

2. On the CyberArk PSM Server you will see in the Airwall Server agent which devices it has been given trust to:
   a. Click on the HIP Networks View icon (network symbol):



Airwall Server Control Panel

96622F459C27

Running

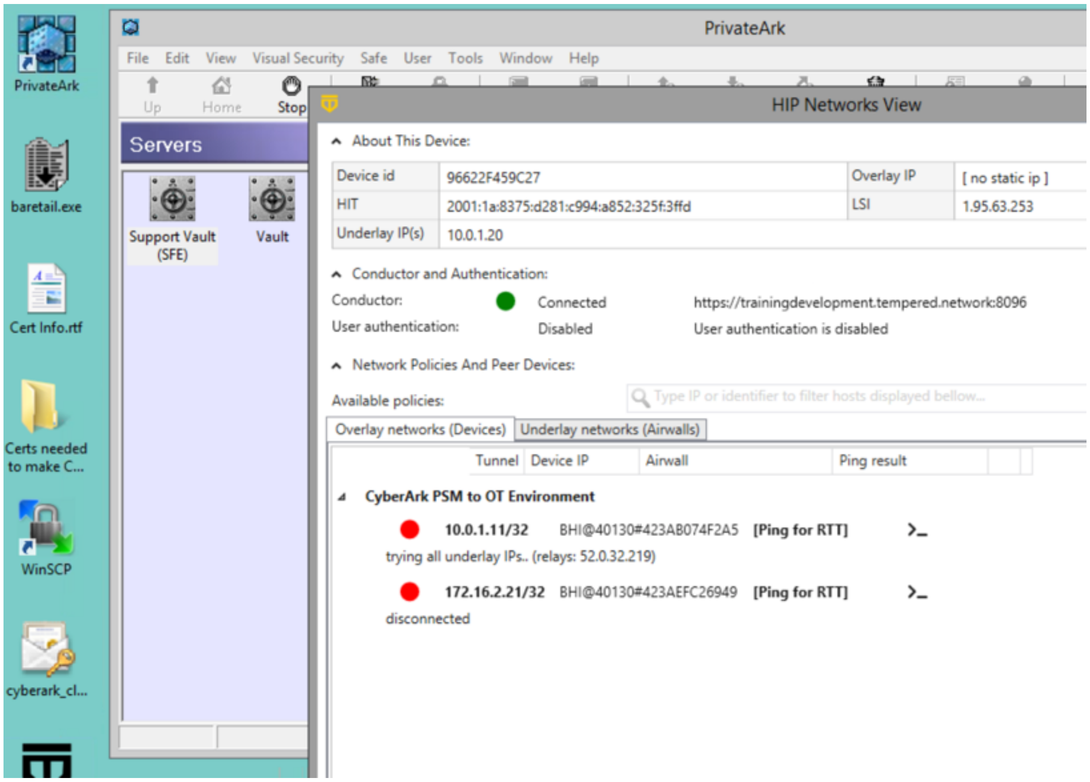
User authentication is disabled

HIP lockdown is off

In split-tunnel mode

Airwall Server, version:2.2.3.651,
Tempered Networks, Inc. 2012-2020

b. HIP Networks View



HIP Networks View

About This Device:

Device id	96622F459C27	Overlay IP	[no static ip]
HIT	2001:1a:8375:d281:c994:a852:325f:3ffd	LSI	1.95.63.253
Underlay IP(s)	10.0.1.20		

Conductor and Authentication:

Conductor: ● Connected https://trainingdevelopment.tempered.network:8096

User authentication: Disabled User authentication is disabled

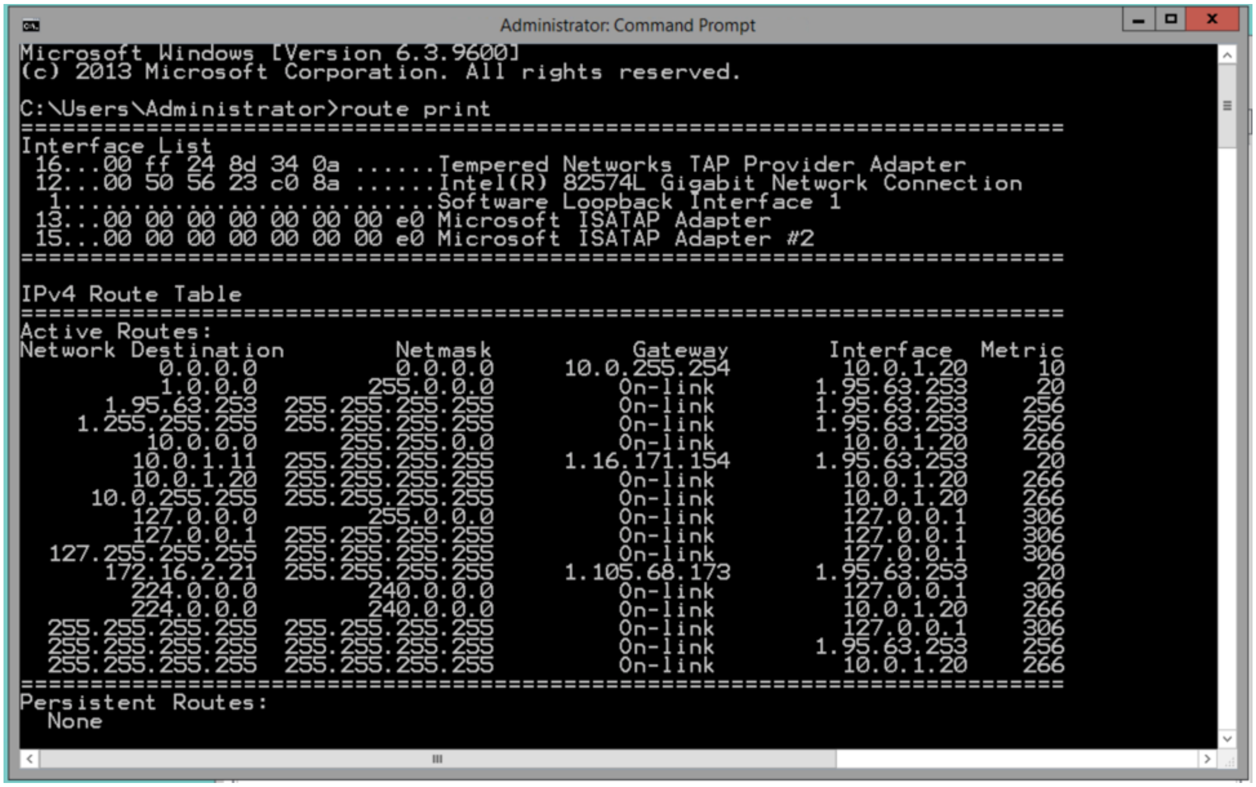
Network Policies And Peer Devices:

Available policies: Type IP or identifier to filter hosts displayed bellow...

Overlay networks (Devices) | Underlay networks (Airwalls)

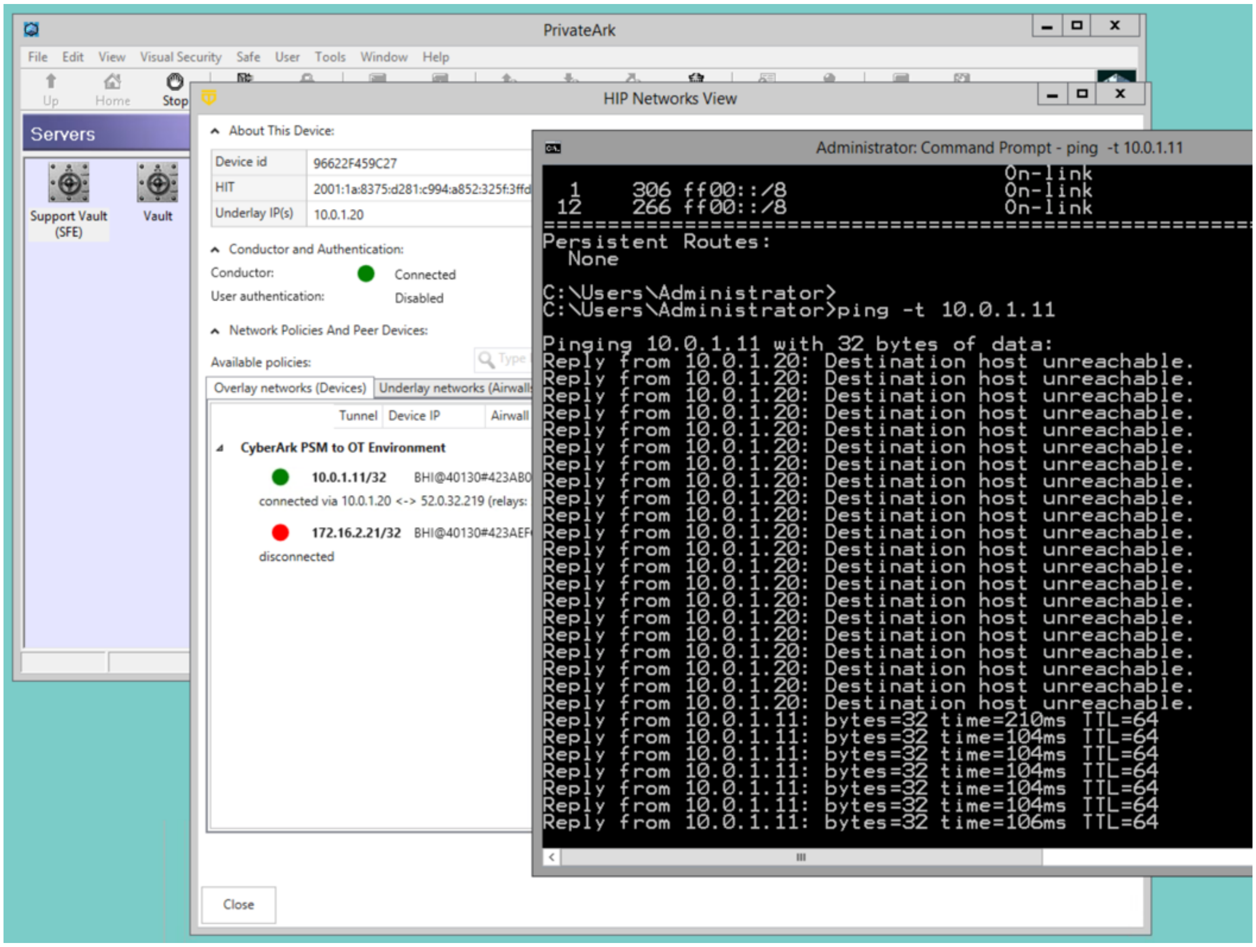
Tunnel	Device IP	Airwall	Ping result
CyberArk PSM to OT Environment			
●	10.0.1.11/32	BHI@40130#423AB074F2A5	[Ping for RTT]
trying all underlay IPs.. (relays: 52.0.32.219)			
●	172.16.2.21/32	BHI@40130#423AEFC26949	[Ping for RTT]
disconnected			

3. In addition, if you look at the route table on the CyberArk PSM server you will see the new /32 routes that have been established in order to send the data to the TAP port (tunnel endpoint).



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>route print
===========================================================================
Interface List
 16...00 ff 24 8d 34 0a ......Tempered Networks TAP Provider Adapter
 12...00 50 56 23 c0 8a ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
 13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     10.0.255.254      10.0.1.20     10
          1.0.0.0        255.0.0.0         On-link     1.95.63.253     20
      1.95.63.253  255.255.255.255         On-link     1.95.63.253    256
    1.255.255.255  255.255.255.255         On-link     1.95.63.253    256
         10.0.0.0      255.255.0.0         On-link       10.0.1.20    266
        10.0.1.11  255.255.255.255     1.16.171.154    1.95.63.253     20
        10.0.1.20  255.255.255.255         On-link       10.0.1.20    266
     10.0.255.255  255.255.255.255         On-link       10.0.1.20    266
        127.0.0.0        255.0.0.0         On-link       127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link       127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link       127.0.0.1    306
      172.16.2.21  255.255.255.255     1.105.68.173    1.95.63.253     20
        224.0.0.0        240.0.0.0         On-link       127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       10.0.1.20    266
  255.255.255.255  255.255.255.255         On-link       127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     1.95.63.253    256
  255.255.255.255  255.255.255.255         On-link       10.0.1.20    266
===========================================================================
Persistent Routes:
  None
```

Note that a tunnel will not be established until traffic is initiated from the CyberArk PSM server to the protected devices. A continuous ping should be started as it may take several minutes for the tunnel to establish through the Relay the first time.


PrivateArk
File Edit View Visual Security Safe User Tools Window Help
Up
Home
Stop
Servers
Support Vault (SFE)
Vault
HIP Networks View
Administrator: Command Prompt - ping -t 10.0.1.11
Close

About This Device:

Device id	96622F459C27
HIT	2001:1a:8375:d281:c994:a852:325f:3ffd
Underlay IP(s)	10.0.1.20

Conductor and Authentication:

Conductor: ● Connected

User authentication: Disabled

Network Policies And Peer Devices:

Available policies:

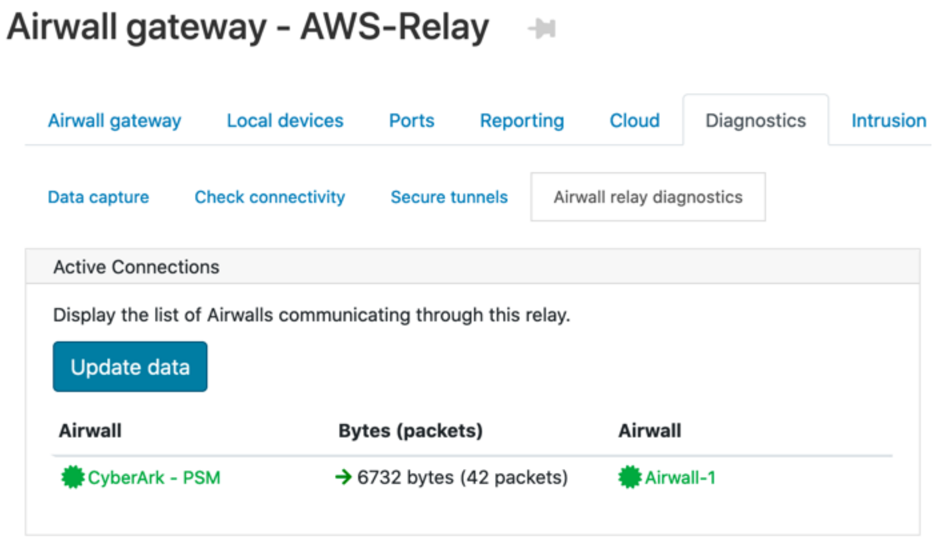
Overlay networks (Devices) | Underlay networks (Airwalls

	Tunnel	Device IP	Airwall
CyberArk PSM to OT Environment			
● 10.0.1.11/32		BHI@40130#423AB0	
connected via 10.0.1.20 <-> 52.0.32.219 (relays:			
● 172.16.2.21/32		BHI@40130#423AEF	
disconnected			

```
                                                      On-link
  1    306 ff00::/8                                   On-link
 12    266 ff00::/8                                   On-link
===========================================================================
Persistent Routes:
  None

C:\Users\Administrator>
C:\Users\Administrator>ping -t 10.0.1.11

Pinging 10.0.1.11 with 32 bytes of data:
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.20: Destination host unreachable.
Reply from 10.0.1.11: bytes=32 time=210ms TTL=64
Reply from 10.0.1.11: bytes=32 time=104ms TTL=64
Reply from 10.0.1.11: bytes=32 time=104ms TTL=64
Reply from 10.0.1.11: bytes=32 time=104ms TTL=64
Reply from 10.0.1.11: bytes=32 time=104ms TTL=64
Reply from 10.0.1.11: bytes=32 time=104ms TTL=64
Reply from 10.0.1.11: bytes=32 time=106ms TTL=64
```

Testing, Diagnostics and Troubleshooting

The Conductor has an abundance of tools for troubleshooting any network scenario including packet captures and packet traces. One of the more important tools for this scenario is looking at the Airwall Relay to see if a connection has been established from the Airwall Server on the CyberArk server to the Airwall Gateway.



Airwall gateway - AWS-Relay

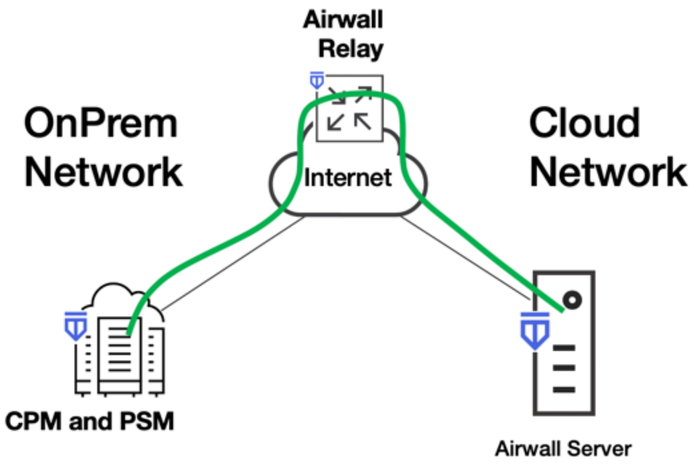
Active Connections

Display the list of Airwalls communicating through this relay.

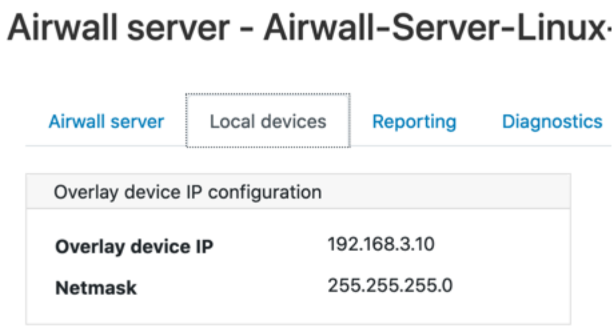
Airwall	Bytes (packets)	Airwall
CyberArk - PSM	→ 6732 bytes (42 packets)	Airwall-1

CyberArk PSM to Cloud Server

Let’s look at a scenario where CyberArk needs to reach out to a server in a cloud environment that is in an isolated VPC with no inbound access set up. In this situation, rather than putting the cloud server behind an Airwall, it may be preferred to just install the Airwall Server agent on this server.



In this example, we will use the Linux Airwall Server. Installation is similar, albeit via the command line. In this case, we need to add an Overlay IP to the Cloud Server so that it is reachable through the Overlay from the CyberArk PSM.

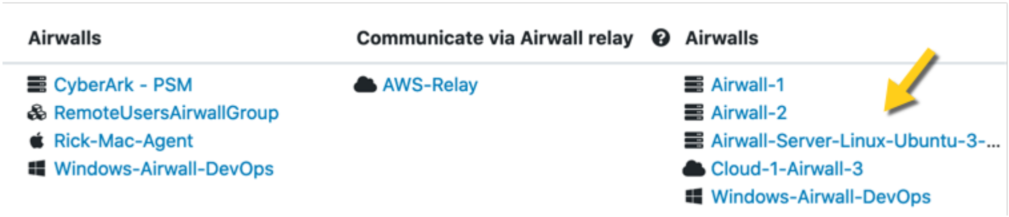


Airwall server - Airwall-Server-Linux·

Overlay device IP configuration

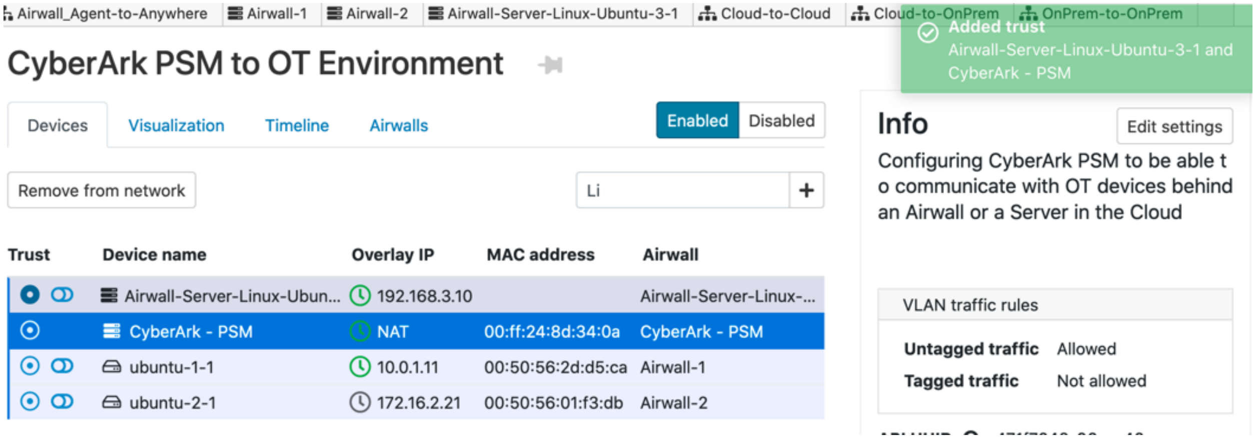
Overlay device IP	192.168.3.10
Netmask	255.255.255.0

Next we need to verify that the Cloud server has relay policy from CyberArk:



Airwalls	Communicate via Airwall relay	Airwalls
CyberArk - PSM	AWS-Relay	Airwall-1
RemoteUsersAirwallGroup		Airwall-2
Rick-Mac-Agent		Airwall-Server-Linux-Ubuntu-3-...
Windows-Airwall-DevOps		Cloud-1-Airwall-3
		Windows-Airwall-DevOps

And finally, we can add the new Cloud Server to the Overlay and assign Trust:



Added trust
Airwall-Server-Linux-Ubuntu-3-1 and CyberArk - PSM

CyberArk PSM to OT Environment

Trust	Device name	Overlay IP	MAC address	Airwall
	Airwall-Server-Linux-Ubun...	192.168.3.10		Airwall-Server-Linux-...
	CyberArk - PSM	NAT	00:ff:24:8d:34:0a	CyberArk - PSM
	ubuntu-1-1	10.0.1.11	00:50:56:2d:d5:ca	Airwall-1
	ubuntu-2-1	172.16.2.21	00:50:56:01:f3:db	Airwall-2

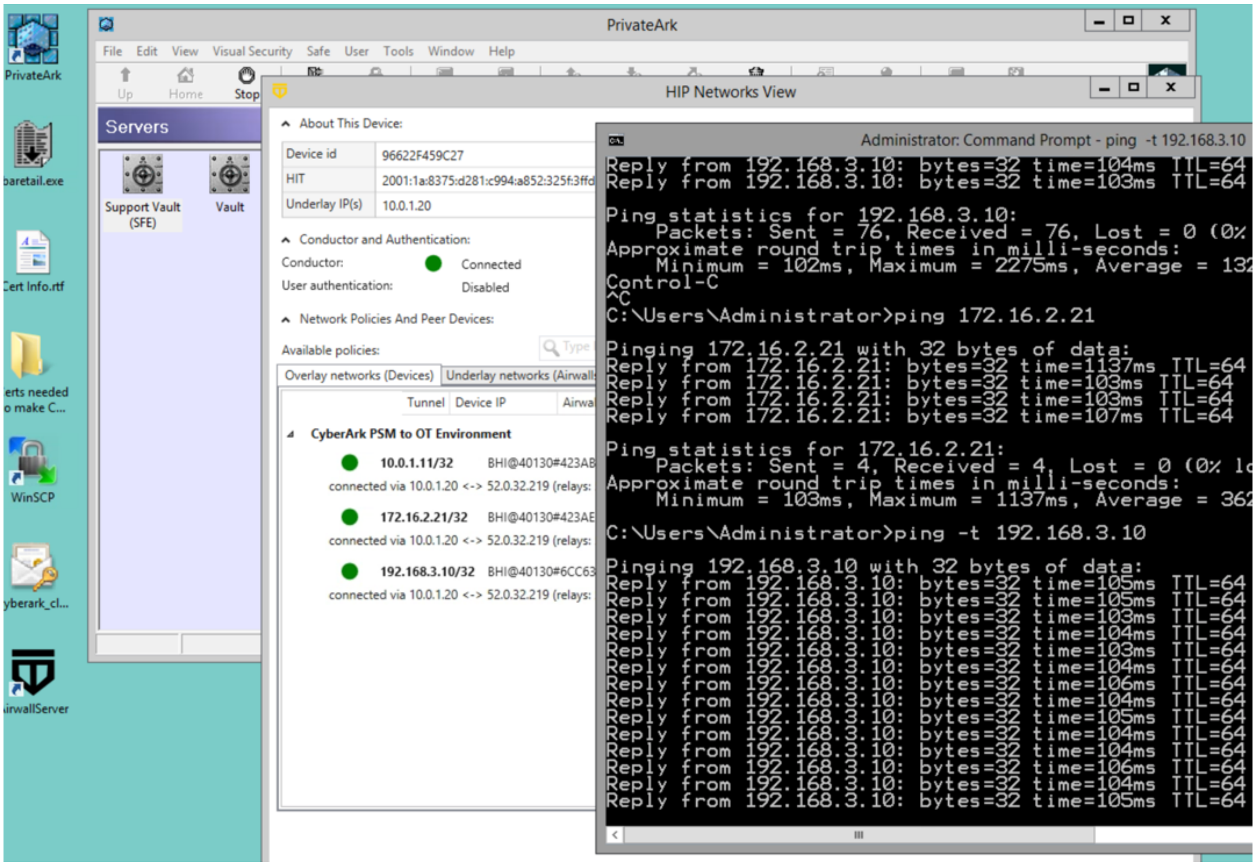
Info

Configuring CyberArk PSM to be able t o communicate with OT devices behind an Airwall or a Server in the Cloud

VLAN traffic rules

Untagged traffic	Allowed
Tagged traffic	Not allowed

Looking at CyberArk PSM, we can see the new Cloud Server and can reach it:



About This Device:

Device id	96622F459C27
HIT	2001:1a:8375:d281:c994:a852:325f:3ffd
Underlay IP(s)	10.0.1.20

Conductor and Authentication:

Conductor: ● Connected

User authentication: Disabled

Network Policies And Peer Devices:

Available policies:

Overlay networks (Devices) | Underlay networks (Airwalls

	Tunnel	Device IP	Airwa
CyberArk PSM to OT Environment			
● 10.0.1.11/32		BHI@40130#423AB	
connected via 10.0.1.20 <-> 52.0.32.219 (relays:			
● 172.16.2.21/32		BHI@40130#423AE	
connected via 10.0.1.20 <-> 52.0.32.219 (relays:			
● 192.168.3.10/32		BHI@40130#6CC63	
connected via 10.0.1.20 <-> 52.0.32.219 (relays:			

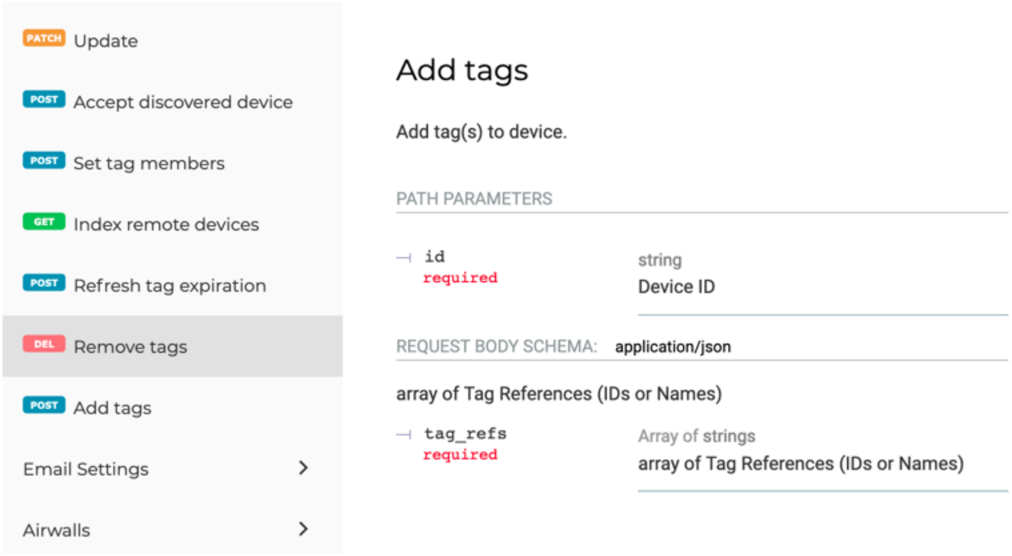
Administrator: Command Prompt - ping -t 192.168.3.10

```
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=103ms TTL=64

Ping statistics for 192.168.3.10:
    Packets: Sent = 76, Received = 76, Lost = 0 (0%
Approximate round trip times in milli-seconds:
    Minimum = 102ms, Maximum = 2275ms, Average = 132
Control-C
^C
C:\Users\Administrator>ping 172.16.2.21

Pinging 172.16.2.21 with 32 bytes of data:
Reply from 172.16.2.21: bytes=32 time=1137ms TTL=64
Reply from 172.16.2.21: bytes=32 time=103ms TTL=64
Reply from 172.16.2.21: bytes=32 time=103ms TTL=64
Reply from 172.16.2.21: bytes=32 time=107ms TTL=64

Ping statistics for 172.16.2.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% lo
Approximate round trip times in milli-seconds:
    Minimum = 103ms, Maximum = 1137ms, Average = 362

C:\Users\Administrator>ping -t 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:
Reply from 192.168.3.10: bytes=32 time=105ms TTL=64
Reply from 192.168.3.10: bytes=32 time=105ms TTL=64
Reply from 192.168.3.10: bytes=32 time=103ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=103ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=106ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=105ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=106ms TTL=64
Reply from 192.168.3.10: bytes=32 time=104ms TTL=64
Reply from 192.168.3.10: bytes=32 time=105ms TTL=64
```

If overlapping IP address space exists in any environments, you can always use a different NAT address for the remote device to avoid conflicts.

Using Tempered's Conductor API

While this integration guide documents a static example of providing access for CyberArk into a protected OT environment, this connection could be dynamic if leveraging the Conductor API. Most Conductor functionality is available via the REST API, so automation of Trust from the CyberArk Server could set up for JIT – just in time, access.



Add tags

Add tag(s) to device.

PATH PARAMETERS

id required	string Device ID

REQUEST BODY SCHEMA: application/json

array of Tag References (IDs or Names)

tag_refs required	Array of strings array of Tag References (IDs or Names)

The following scenario could be configured. An Alero user connects to CyberArk for access to a Protected device. CyberArk validates the user using biometric, multi-factor authentication via the Alero web portal. When Alero contacts the Core Privileged Access component within CyberArk, it could dynamically reach out to the Conductor API and simply assign a Tag to the Airwall Server to provide access. When the user disconnects the Tag can be removed and persistent access is no longer required, reducing cybersecurity exposure.