Alignment with ACSC ICS Remote Access Protocol

Framework Mapping to
Australian Cyber Security Centre

DISPEL

Dispel's Alignment with ACSC ICS Remote Access Protocol

Introduction

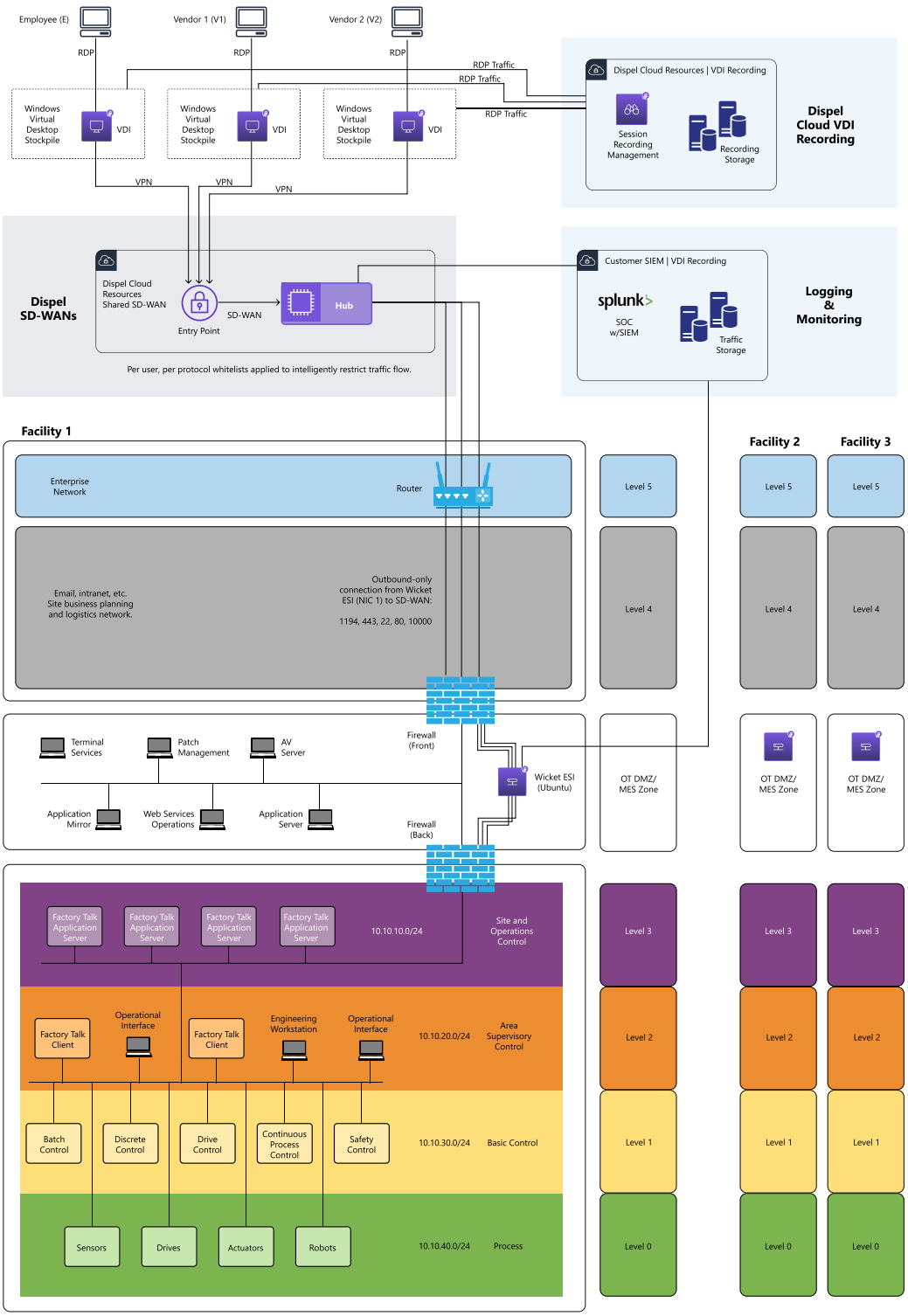
Industrial automation and control system ("IACS") organizations increasingly use commercial off-the-shelf ("COTS") networked devices that are inexpensive, efficient, and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies, and increased connectivity elevate the theoretical cyber risk of control system hardware and software. This, in turn, has raised concerns over Health, Safety and Environmental ("HSE"), financial, and/or reputational consequences from cyberattacks on deployed control systems.

The ACSC ICS Remote Access Protocol is not a prescriptive guide. The goal of the document is to provide a flexible framework that *facilitates* addressing current and future vulnerabilities in IACSs and applying necessary mitigations in a systematic, defensible manner.

This document begins with a brief architecture overview of Dispel Remote Access, then details how Dispel's remote access solution meets and exceeds each design guideline put forth by the ACSC ICS Remote Access Protocol.

Dispel Architecture Overview

Purdue Model Diagram of Dispel Deployment



Components

Dispel Wicket ESI

Bottom third of diagram, Layer 3.5 of Purdue Model (OT DMZ)

The Dispel Wicket ESI is an on-premises remote access gateway that can be deployed as either hardware or a virtual appliance. It contains two network interface cards: North, and South. North connects outbound-only through a single port to a single IP to establish a remote access pathway through the SD-WAN, and South is given routability to devices on the OT network. On-premise firewalls can control the North and South sides independently to maintain strict need-based access and network segmentation. The Wicket ESI is the only on-premise installation required, and enables secure remote access to any device permitted on the South side network.

Dispel SD-WANs

Grey box on upper left, cloud-based core network

The Dispel SD-WAN is the main bridge enabling remote access. The Wicket ESI proactively connects from one side of the SD-WAN, and on the other side, the Virtual Desktops are automatically networked in. Each Dispel SD-WAN is single-tenant to each customer, meaning your traffic and another customer's traffic will never traverse the same infrastructure. Additionally, Dispel SD-WANs are built with Moving Target Defense technology, enabling a shifting topology and increased resiliency.

Dispel VDIs (Virtual Desktops)

Top of diagram, cloud-based workstations

Dispel Virtual Desktops (VDIs) are single-use, time-limited workstations that users connect through to access the ICS network. Virtual desktops can be set to automatically cycle on an administrator-defined schedule. This ensures that each desktop is never used for more than 12 hours, and all valid credentials for remote access are cycled every 24 hours. Virtual desktops that connect to your ICS network will never connect to another network or another country. Lastly, virtual desktops will automatically build with the latest updates and patches to the day, and can be customized and imaged with your desired applications and security policies.

Dispel Logging and Recording

Blue boxes on the upper right, cloud-based add-ons

All access performed through Dispel is recorded in two ways:

1. Syslog traffic packets which contain the user, timestamp, what devices the user accessed, and through which protocol. Dispel can provide an integrated server to store these logs as part of the managed deployment, or the traffic can be forwarded to a customer's existing SIEM (eg. Splunk).
2. Full video screen recordings of each Virtual Desktop session. Recordings can be watched in real-time, and are saved for playback. Videos can be retained for an administrator-defined period of time, stored permanently, or exported. Dispel can provide a recording storage server to enable this functionality with no additional hardware needed from the customer.

Point-by-point Guideline Mapping

Requirement		Principle	Dispel Product/Feature	
Design	**1**	By default, there should be no communication between the vendor and the critical infrastructure control system.	By default, there is no communication possibility between the vendor and critical infrastructure. Access credentials are refreshed from session to session, ensuring the prevention of lingering or unwanted communication is. This is enforced at multiple levels: - No direct access. All connections must go through a hardened virtual desktop acting as an intermediary. - Vendors start from a suspended-by-default state, and must complete a "Request Access Form" for their account to gain access to a single-tenant, locked-to-them virtual desktop. Access is granted only for the time window allowed by the administrator. - The remote access network may be destroyed when not in use.	Yes
Design	**2**	Networks should be segmented and segregated. Details on the application of segmentation and segregation can be found in the ACSC's *Implementing Network Segmentation and Segregation* publication. Included in this process will be firewalls. The firewalls should be configured as tightly as possible, including restricting to specific protocols, ports, MAC and IP addresses, and directions. For example, a stateful firewall could be employed which allows communication to be initiated only in one direction. Internet-facing firewalls and the control system de-militarised zone (DMZ) firewall should be completely separate devices.	Dispel's on-premises remote access gateway, which we call a "Wicket ESI" has two segmented network interfaces. - The North interface establishes an encrypted, outbound-only connection to the single-tenant Moving Target Defense (MTD) network, which we call a Dispel Enclave. This connection requires a single outbound-only firewall rule to a single IP address, through a single port. - The South interface provides gateway access to the OT environment. The Wicket is deployed in the OT-DMZ between the internet facing firewall (for the North network interface) and the separate OT firewall (South network interface). No inbound firewall rules are needed from the Internet, and no devices on the control system need direct Internet access.	Yes

Design	**3**	There must be other processes and procedures in place before this protocol is used. These processes include: - A way to disconnect the control system from the internet quickly, if unwanted external control or actions are detected. - A way to revert the control system to a known good state. - A cyber-incident response plan in case malware is introduced. - The expected safety plans, in case an unwanted physical action took place.	Dispel provides this functionality in a number of ways. - Dispel helps detect incidents through session recording and traffic logging/monitoring. These help a customer gain visibility into their environments. - Administrators may instantly delete Virtual Desktops suspected of malicious behavior. This allows the rest of the network to function normally while severing an isolated virtual desktop and disconnecting an unwanted user from the control system instantly. - Administrators may destroy the MTD remote access network on-demand if necessary. This would remove any potential for external connectivity and return the OT environment to a fully offline state. - Administrators may destroy the Wicket Virtual Machine (if virtual appliance) or unplug the Wicket's ethernet cables (if hardware appliance) as a secondary method of ensuring no possibility of external connectivity.	Yes
Design	**4**	Multi-factor authentication should be used. Two-factor authentication should be used at a minimum. Details, including why this is needed, can be found in the ACSC's *Implementing Multi-Factor Authentication* publication.	Multi-factor authentication is enforceable at an organization level for all users on the Dispel platform. We support temporary one-time passwords (ToTP) or hardware tokens such as YubiKeys. We also have a number of SSO integrations with Active Directory, Microsoft, OAuth2.0 providers like Okta, and SAML.	Yes

Design	**5**	Ensure the login credentials are such that a specific person at the remote end is attributed to the actions, rather than a generic login for an organisation. Ensure these person-specific details are recorded, for example in an Access Log or Engineering Change Request.	All Dispel logins are created on a per-user basis, whether through our login process or SSO. Further Multi-factor Authentication is used to further associate a user to their account. Vendors must also fill out an access request form wherein they provide their identity, reason/scope for access, and the time window they need to complete the task. This request must be approved by an authorized party and the request + approver are documented for auditing purposes.	Yes
Design	**6**	Time limit the connection (e.g. to 24 hours or the length of a shift) and ensure the credentials are one-time-use credentials. Ensure the credentials expire after 24 hours whether they are used or not.	All virtual desktops are built with one-time-use credentials and Administrator-defined time intervals. We recommend 12-hour shifts, and that any unused Virtual Desktops are automatically cycled every 24 hours. Thus, all active connections are limited to 12-hour sessions, and all unused desktop credentials expire after 24 hours automatically.	Yes
Design	7	If the connection is inactive for more than 30 minutes, the connection should be removed. 30 minutes may be restrictive, if processes essential to the task such as firmware updates take longer than 30 minutes. If longer is required, a case should be put forward and relevant records kept.	Virtual Desktops automatically time out after 15 minutes of inactivity. This time limit is admin configurable. Configuration customizations like this are documented and delivered to the customer.	Yes
Design	**8**	Ensure there is a procedure to acquire approval for connection of remote access by a senior officer of the organisation. If there are particular necessary notifications in various jurisdictions, list them here.	Dispel can be configured to require access requests for every session through a built-in Request Access Form. The Request Access form automatically sends incoming requests to a defined list of senior officers / administrators. By default, only administrators of the remote access network and the relevant facility in question can approve Request Access Forms. In addition, an administrator may not approve their own request. For specific jurisdictions, administrators may delegate approval responsibilities to others. That list of approvers is only editable by those with administrator permissions, and is documented within the console.	Yes

Design	**9**	Ensure the device used at the remote (vendor) end is used solely for the purpose of connecting to the Australian critical infrastructure organisation. That is, the computer at the remote organisation cannot be used to connect to country X yesterday, country Y the day before, Australia today, and country Z tomorrow. The preference is to use a laptop at the vendor's end provided by the Australian Critical infrastructure organisation, rather than relying on third party infrastructure. The computer should only be used for connecting to Australia's critical infrastructure organisations, for the purpose of accessing the control system once through the various internal connections. One computer at the remote organisation dedicated to one Australian organisation is the ideal, and if this ideal cannot be met explain how you are going to mitigate the risk.	By using virtual desktops as disposable intermediate hosts, customers can ensure that: - The virtual desktop used to complete the work was built for the explicit purpose of connecting to only the one Australian critical infrastructure needed to complete that scope of work. - The same virtual desktop will never be used across multiple countries or organizations. Each virtual desktop is allowed to connect to only one ICS environment, ever. - Vendors are never directly connecting to the ICS environment. All desktops that connect to the ICS environment will only connect to this specific ICS environment in its lifetime.	Yes
Design	**10**	Apply ASD's 'Top Four' to the highest maturity level, with the rest of the 'Essential Eight' where applicable on the computer at the remote end. It is noted that the process of managing a standalone computer by the remote organisation will be challenging.	By using customer-controlled virtual desktops, they can ensure that: - [Mitigation 1] Only allowed applications are on the virtual desktop image. No additional application downloads are permitted. - [Mitigation 2] Applications on the virtual desktops are patched to their latest versions. - [Mitigation 3] Virtual desktops and remote access infrastructure is automatically patched at build and during its lifetime. - [Mitigation 4] Privileges are scoped only to the specific devices they need access to and administrative privileges are not available on the virtual desktops. These mitigations comprise the ASD's "Top Four". In addition, Dispel helps customers with multi-factor authentication, controlled use of application and endpoint hardening, and regular backups/disaster recovery to round out the Essential Eight.	Yes

Design	**11**	Apply ASD's 'Essential Eight' where applicable on all interim machines internal to the critical infrastructure organisation's network that are not prevented from such measures for OT reasons. Example computers that could have their security improved in this way include machines in DMZs and jump boxes in general, and any machine used by the CI organisation to view, control or supply credentials to the vendor's connection. Examples of what 'where applicable' covers is that if Microsoft Office is not installed, then macros may not be an issue; and if no data is locally stored, daily backups may not be unnecessary.	Dispel's remote access platform is fundamentally different in that the customer, not the end vendor, will control the virtual desktops. Therefore all applicable measures desired in the ASD's 'Essential Eight' can be applied by default.	Yes
Design	**12**	'Bastion hosts' (special-purpose computers on a network specifically designed and configured to withstand attacks) and interim machines should be turned off whenever possible, when not in use to prevent attackers acquiring a foothold while the remote vendor protocol is not in use, and waiting for a connection to the internet. Having machines turned off when not in use will add complexity to the requirement to maintain the 'Top Four' and 'Essential Eight', so a plan needs to be created to manage this.	Dispel employs disposable virtual infrastructure, which can be turned off when not in use to prevent attackers from acquiring a foothold. Further, these virtual desktops are cycled regularly and change on a daily basis, allowing connections for authorized users while preventing enemies from gaining footholds into the OT environment. Dispel's principle service is the orchestration and management of these virtual machines, so we will deliver a fully functional plan to customers during the deployment.	Yes
Design	**13**	To aid in mitigating the risk of supply chain attacks, critical infrastructure operators and vendors should put in place robust mechanisms to verify all software and tools used in the remote vendor access protocol process. This includes the engineering analysis and fault investigation tools.	As the owner of the virtual desktop image, the customer may review all software and tools used in the remote access process. Further, Dispel helps provide visibility by enacting port and protocol traffic monitoring, as well as full recording of virtual desktop sessions.	Yes
Design	**14**	Ensure contractually that any data viewed or acquired as part of the remote access is used only for the purpose of resolving the issue the remote access was granted for, and must be returned to the critical infrastructure organisation and destroyed at the remote access end either when the issue is resolved, or after the period of 1 year, whichever is sooner.	As all work is completed within the virtual desktop environment, so all associated data never needs to leave the controlled scope of the customer. That said, we advise customers to include relevant language in their contracts.	Yes

Design	**15**	Ensure contractually that there is an ability to audit the organisation at the remote end to ensure each of the conditions is met. These conditions include 'device only used for Australia', device has had ASD's 'Essential Eight' applied where applicable, data is kept only for as long as it needs to be and a copy of what was obtained is returned to the critical infrastructure organisation, etc. Also explicitly looked for should be the applicable cipher suites available at the vendor's end, such that the risk of a down-grade of cipher-suite attack is managed.	Virtual desktops are programmatically scoped to only the organization, and are built from customized golden images to comply with Essential Eight rules. End-to-End encryption is provided using AES-256 with 4096 bit RSA. Although Dispel mitigates these risks, we advise customers to include relevant language in their contracts to fulfill this design principle.	Yes
Design	**16**	Ensure contractually that there is ability to periodically red-team test the protocol at all parts of the protocol, including the remote vendor's end.	Dispel undergoes periodic penetration testing from HackerOne, and customers are allowed to perform their own penetration testing under the appropriate instances.	Yes
Design	**17**	Ensure contractually that any connectivity and hosting requirements for the remote access infrastructure is specified. That is, consider the ability to perform denial-of-service attacks against the remote vendor protocol, and the impact of this to the critical infrastructure organisation in an emergency.	Dispel has a number of procedures and policies in place to mitigate denial of services attacks. - The remote access network itself has all ports and protocols turned off, except for those explicitly allowed for individual components to work together. - Virtual Desktops allow RDP connections from only the approved user, and only after they've been granted an access window. - Dispel employs regional resiliency measures to quickly recover from datacenter/cloud-level outage events. - The front-end console mitigates DDoS attacks with techniques including TCP Syn cookies and connection rate limiting. The console also maintains a multiple backbone connection architecture with internal bandwidth capacity that exceeds the internet carrier supplied bandwidth. In the event of a DDoS attack, our console hosting platform enables additional advanced DDoS mitigation controls where needed.	

END

About Dispel
Dispel supplies secure remote access platforms for industrial control systems. Dispel serves over 12 million people and partners from offices in New York, Austin, Boston, Denver, Virginia, and Tokyo.

Dispel, LLC
61 Greenpoint Ave,
Suite 634
Brooklyn, NY 11222

dispel.io

For more information
enterprise@dispel.io
+1-917-268-5190

Printed April 11, 2022