Understanding Comply-to-Connect (C2C)

And U.S. Department of Defense requirements

Overview

At Cisco we believe empowering our nation's defenders through innovative technologies is key to securing the homeland. This includes helping our partners in government better understand U.S. Department of Defense (DoD) and MILDEP specific policies for information assurance. So we would like to familiarize our DoD customers with Cisco Security solutions that can be deployed as part of a Comply-to-Connect (C2C) architecture, and to present our recommendations for comprehensive C2C capabilities.

The primary goal of C2C is Network Access Control, and requires five critical capabilities:

- Controlling and verifying the identity of users and devices before network access is granted
- Limiting access to resources, based on policy and authorization
- Visibility into who and what is connected to your network, while providing continuous monitoring
- Prevention and control of malicious activities, such as propagation of malware, that can lead to denial-of-service, network infiltration, and data exfiltration
- Automating the response to breaches and remediation of vulnerabilities.

© 2018 Cisco and/or its affiliates. All rights reserved.

How C2C helps

The Cisco C2C solution uses a standards based, security architecture that provides our nation's defenders with the tools they need to protect and secure a network, regardless of user and device location and access method.

C2C is built upon industry standard protocols, such as IEEE 802.1X, and empowers you to make the right choices about who connects to your network. It also uses Cisco's powerful Identity Services Engine (ISE) that now integrates with ACAS, McAfee ePO and other existing DoD tools to automate NAC and posture assessment.

Cisco C2C also helps you futureproof your network and is a core component of the Cisco DNA modernization solution. Plus it is critical to a Software Defined Access (SDA) solution.

With C2C, DoD agencies like yours can meet the following:

- Compliance with Security Technical Implementation Guides (STIGs)
- Compliance with DoD Instruction 8420.01, "Commercial WLAN Devices, Systems, and Technologies"
- Compliance with Defense Information Systems Agency (DISA) and DoDIN Unified Capabilities Requirements
- Compliance with MILDEP specific network functional specification
- Support for 802.1X with extensible authentication protocol (EAP)
- Compliance with Federation Information Processing Standards (FIPS) and Common Criteria encryption standards.

Cisco also supports the Radius Change of Authorization (CoA) feature that can dynamically change user and device access after the initial authentication, authorization, and posture assessment, assuming endpoint status changes.

© 2018 Cisco and/or its affiliates. All rights reserved.

Securing our nation's defense networks

Today's DoD networks make up the core of the command and control infrastructure that provides our nation's defenders access to the mission-critical services they need to maintain operations and complete their missions. They must also provide access to users from anywhere in the world while supporting various access methods via wired, wireless, and VPN. As a result, the traditional network perimeter has expanded beyond the standard top-level-architecture (TLA) that we are used to, with no single product able to defend against vulnerabilities and attacks. These networks must be secured using an architecture approach. A C2C solution should be the foundation on which a solid security architecture and posture is built on.

The need for greater network visibility

IT modernization has now become a key focus of the DoD. In response, they have developed programs to help improve operational efficiencies and reduce the attack surface, all while enhancing security. But it is increasingly clear that the DoD must have continuous visibility into their networks to help better protect it before, during, and even after an attack. As a result, it is critical to empower our defenders with the tools to:

- Use sensor and telemetry data to gain visibility into all users and devices that are connected to DoD networks, 24/7
- Authenticate network access and determine the security posture status of users and devices and control access based on policy and authorization
- Continuously monitor activities via anomaly detection and machine learning mechanisms
- Use Cloud and on-prem tools as intelligence sources
- Automate the response to attacks and perform remediation actions such as quarantine and patching.

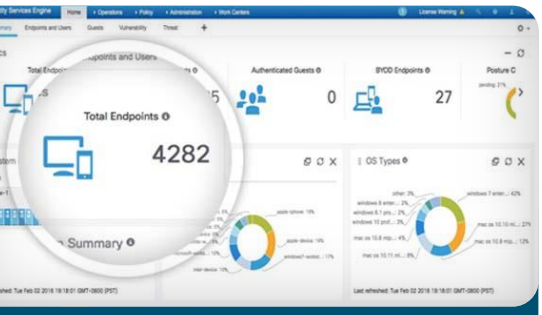
What a C2C architecture provides

1. Verification of the identity of all users and devices

With potential threats increasing against our nation, granting network access to any user and their device, before authenticating, is risky. Why? Because:

- The device might not be government-owned
- Even if the device is permitted, it might not have the latest operating system patches, exposing the network to risk from malware, virus propagation, and denial-of-service attacks
- Any user who connects with a device could potentially access data and applications without detection
- The device might be infected with malicious software.

The DoD currently uses a variety of access-control methods, including port-based security, to control device access. But this requires cross-checking the device's MAC address against a manually created list of authorized addresses. And port security doesn't scale and requires manual configuration. Plus MAC addresses can be spoofed.



Two key solutions

Cisco Identity Services Engine

Our Identity Services Engine (ISE) lets you see and share rich user and device details via a simple, flexible interface. It also lets you control all access from one place and simplifies access across all your network's wired, wireless, and VPN connections.

Plus, it can help you reduce risks and contain threats by dynamically controlling network access. ISE can also assess vulnerabilities and apply threat intelligence, or even contain a suspicious device for remediation. Find out more at: http://cs.co/ISEforDoD.

Cisco Stealthwatch

Stealthwatch helps you keep unauthorized users and devices from accessing restricted areas of your network. And it stores telemetry data for longer periods, while using advanced analytics.

Our Stealthwatch solution also lets your team extend visibility and control to your data center and the cloud to secure workloads in Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure. Learn more at: http://cs.co/DoDStealthwatch.

© 2018 Cisco and/or its affiliates. All rights reserved.

MAC authentication bypass (MAB) can help overcome these port-security issues to some extent but doesn't fully satisfy C2C requirements because it doesn't validate the device's security posture. It is also unable to control access based on user identity, device type, or device location. Overhead is also high because the network administrator must manually maintain a list of MAC addresses that are authorized for network access.

By enabling your network to see and share the details of every connected device (through device profiling), and automating the collection and maintenance of the MAC list, you can overcome these issues. So any C2C solution should do the following:

- Profiling - create device profiles containing:
  - Device ownership (so that only permitted devices are allowed)
  - Device type (to determine network use, e.g. printer, IP phone)
  - Manufacturer (useful for inventory reports, upgrades)
  - Operating system
- Dynamically profile devices to collect/maintain a MAB database to reduce manual errors.

2. Prevention of unauthorized and/or compromised endpoints from accessing the network

Malware and other malicious software can lead to denial-of-service attacks, network infiltration, or data exfiltration. To mitigate the threat, the network should authenticate and access the endpoint's security posture before allowing it to connect, and automatically remediate non-compliant devices. Your network also needs to have the intelligence to treat different devices appropriately. For example, one version of an operating system might be denied access in most cases but permitted within a highly controlled environment—such as for a critical medical device or aircraft support system.

To help make sure devices connect only when and where they are authorized to, your C2C solutions should be able to:

- Authenticate the endpoint and determine if a device complies with the security posture (security profile should include latest operating system patches and antivirus software)
- Automate remediation (be able to quarantine noncompliant devices and remediate quickly with minimal user effort; saving time and improving productivity)
- Create custom profiles for proprietary systems and devices unique to defense (such as aircraft maintenance systems).

3. Control the user's access to resources, based on policy and authorization

Not all authorized users may need access to all the resources on a network, such as payroll or personnel data. Currently, the DoD controls this access by matching Common Access Card (CAC) credentials to Active Directory. This works fine in a Windows server environment but creates issues for workstations using other operating systems, scanners, and printers.

Also Active Directory does not protect against data exfiltration, man-in-the-middle attacks, and denial-of-service attacks. So we encourage using the Cisco C2C solution along with Active Directory to authenticate users/devices and provide segmentation by deploying solutions that empower:

2017 Winner: Trust Award
Cisco Identity Services Engine

Best Network Access Control (NAC) Solution
SC Security Industry Magazine

C2C means solid cybersecurity

Cisco C2C provides industry-leading cybersecurity that empowers the DoD with end-to-end protection before, during, and after an attack:

- **Before an attack** we help you see what's on your network, set up access controls, enforce security policies, and block applications and access to critical assets
- **During an attack** we help you detect and block them across your networks, endpoints, mobile devices, and virtual environments
- **After an attack** we quickly determine the scope of the damage, remediate it, and help bring your operations back to normal as quickly as possible.

Next steps

To take your agency's next steps to a successful C2C solution, contact us at 1-800-553-6387 or visiting https://cisco.com/go/DoD.

© 2018 Cisco and/or its affiliates. All rights reserved.

- Network awareness by authenticating the user and device then connecting the appropriate VLAN or VRF (guest VLAN = Internet access only while all other VLANs access all or subsets of DoD resources)
- Access control lists (ACLs) for wired, wireless, and VPN connections (grants access based on user's specific identity and permissions, after authentication)
- Scalable group tags (SGTs) that allow administrators to centrally control access to resources (SGT allows network devices to enforce policy and permit/deny traffic accordingly).

4. Context: know the "who, what, where, and when" of your network connections

Network access control is critical—and required—to comply with STIGs, Command Cyber Readiness Inspections (CCRI) and other security audits. Knowing the context of who, what, where, and when for network connections increases situational awareness for your defenders and can aid in investigations by documenting the identity of a user and device generating network traffic. Plus, it can provide you detailed asset information, including which components are nearing end of life. To maximize situational awareness for your network, your C2C solutions should enable:

- Flexible reporting options with the ability to sort devices by manufacturer, operating system version, antivirus software version and more
- Context of device connections that document each connection attempt, including user identity, device, location, time of day, and type of network connection (wired, wireless, or VPN)
- Built-in visibility, eliminating the need to purchase a separate application, lowering costs and reducing deployment issues.

5. Reduction in operating cost by using automation

Using external intelligence sources along with analytics and automation tools is critical to help offload trivial tasks from the cyber-defender so they can focus on more advanced tasks. By automating the NAC, detection, and remediation response processes, you can greatly reduce the time required to maintain your security posture and respond to threats. An example of this is implementing 802.1x and posture assessment during the network access process. By eliminating the need to manually create and maintain a list of authorized MAC addresses for MAB, you can free your team to focus on more critical issues. So your C2C solutions should have the following capabilities:

- Automated network admission control and port security
- Automated device profiling
- Automated application of security patches when a device connects
- Device consolidation (fewer devices mean lower space, power, cooling, and management costs so seek ways to combine your user and device authentication, guest access support, mobile device management (MDM), and bring-your-own-device (BYOD) integration)
- Simplified deployment and operation (remember, automation lowers costs, reduces errors, and frees your high-value team members to focus on more critical work).

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/ trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
USPSDoD-20171122-WP 01/18