Aruba Education Services

Implementing Aruba Network Security

Learner Guide, Volume 1

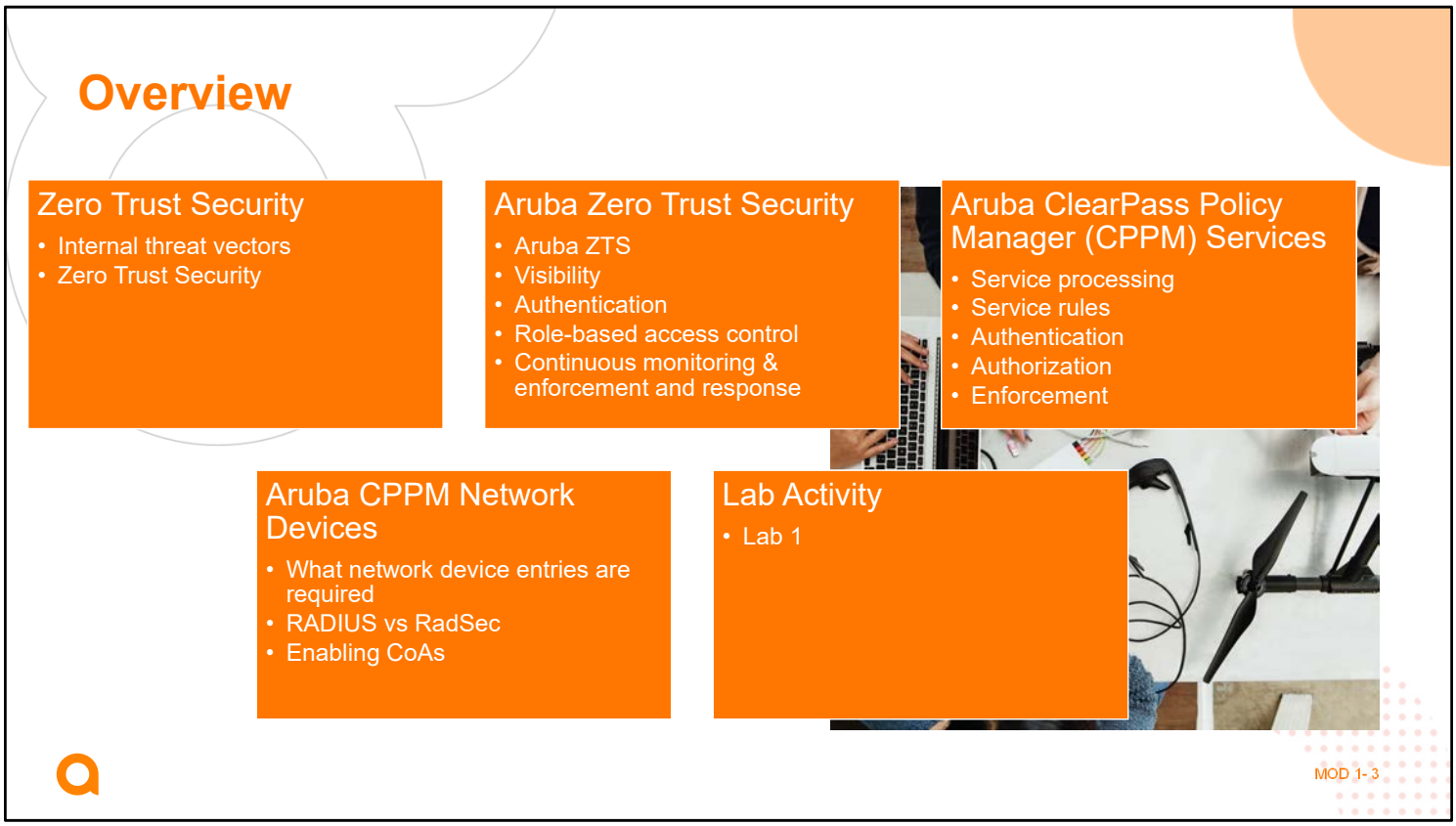
SEPTEMBER 2021

Module 1: Aruba Security Strategy and ClearPass Fundamentals

Objectives

- Explain Aruba Zero Trust Security
- Explain how Aruba solutions apply to different security vectors

By the end of this module, you will be able to explain the Aruba Zero Trust Security strategy. You will also be able to explain how Aruba solutions apply to different security vectors.



In the first topic, you will learn about Zero Trust Security. You will first learn about the pressures that are pushing companies toward a new security approach. You will then learn what Zero Trust Security is and how it helps companies meet their challenges.

In the second topic, you will learn specifically about Aruba Zero Trust Security. You will learn about Aruba's approach to Zero Trust Security, and the Aruba Zero Trust Security components, including visibility, authentication, role-based access control, continuous monitoring, and enforcement and response. You will see how Aruba solutions work together to deliver these features. You will then complete an activity in which you practice presenting the Aruba Zero Trust Security strategy.

You will then examine Aruba ClearPass Policy Manager (CPPM) in more depth, as a foundational piece of Aruba Zero Trust Security. What you learn about creating CPPM services, as well as setting up network device entries on CPPM, in these topics will lay a foundation for the next several modules in this course. You will also view a CPPM service in your lab environment and analyze what the service does.

Topic 1: Zero Trust Security

Why Perimeter Security is No Longer Enough

Traditionally, companies have focused on perimeter security, which uses appliances such as firewalls and Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) to create a secure perimeter around the network. Perimeter security defines zones, including the untrusted, external zone of the Internet and the internal, trusted zone of the corporate LAN.

However, in the modern cyber security landscape, perimeter security alone is hardly enough. Threats can arise from many internal vectors as well. If a company focuses all of its efforts on preventing attacks from outside, and few efforts on controlling behavior from inside, then once hackers have infiltrated the network, they can proceed to wreak havoc.

Common Internal Threat Vectors

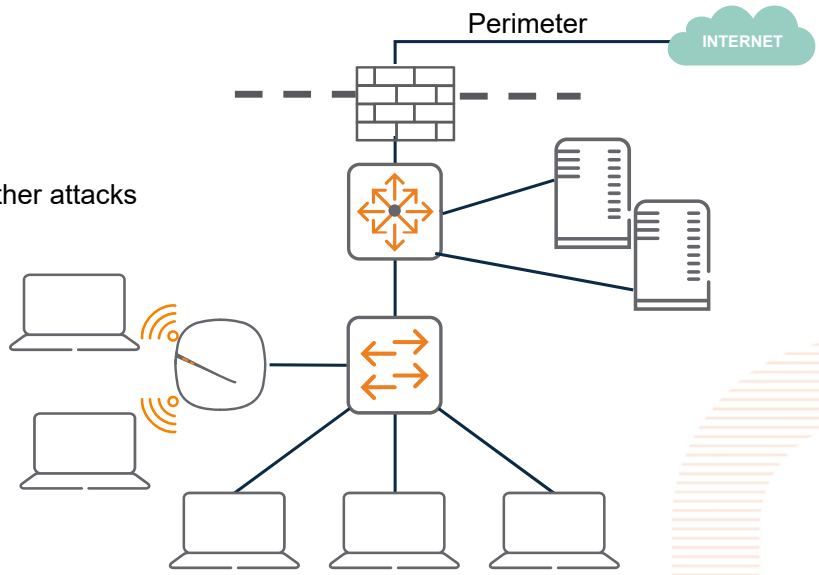
Internal Users

– Malicious employees

– Negligent admins or users

– Shadow IT

– Users who fall for social engineering and other attacks



MOD 1- 6

First companies should be aware that internal users are not always worthy of trust. Malicious employees might launch attacks. Or negligent employees might improperly secure resources, leaving those resources vulnerable to compromise. The Ponemon Institute found that organizations lose, on average per year, 11.45 million USD due to both criminal insiders and employee negligence (https://www.ibm.com/downloads/cas/LQZ4RONE).

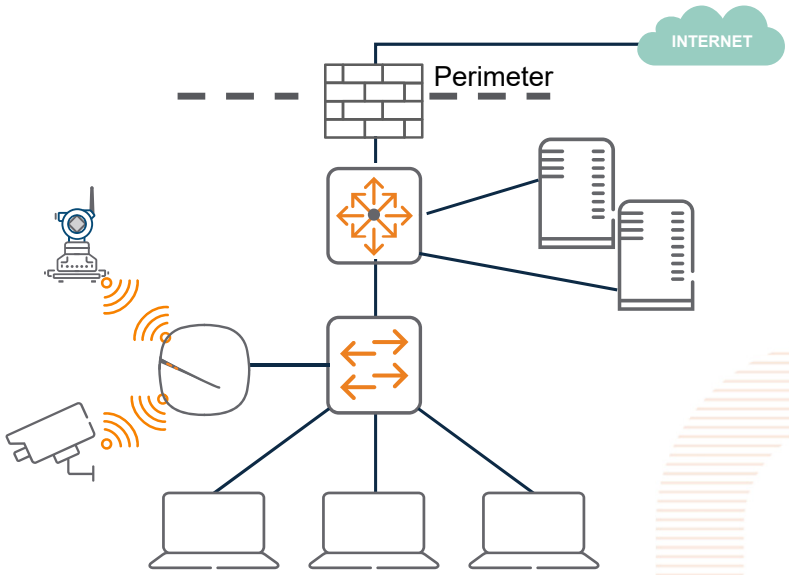
Users might also introduce “shadow IT,” which refers to any unauthorized IT resources deployed by users on their own. For example, users might want wireless access in an area where the company does not allow it, so they add their own AP. Shadow IT creates vulnerabilities because users rarely understand how to deploy resources in a secure way. Returning to the example of an unauthorized AP, hackers can take advantage of an insecure AP to gain access into the corporate LAN from outside the building. In any case, when users deploy shadow IT, they are circumventing policies put in place for a reason and potentially creating vulnerabilities.

Bad actors can also evade perimeter security controls by targeting employees with social engineering, which relies on manipulating individuals rather than penetrating technical defenses. The average cost of a social engineering attack, according to SecurityInfoWatch.com, has risen to 130,000 USD (https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses#:~:text=On%20average%2C%20social%20engineering%20attacks,parties%20or%20new%20cybersecurity%20software).

Common Internal Threat Vectors

IoT

– Increasingly common
  – 55 billion IoT devices by 2022
– Widely insecure
  – Attacked within 5 minutes on average
– Backdoor to more valuable resources



MOD 1- 7

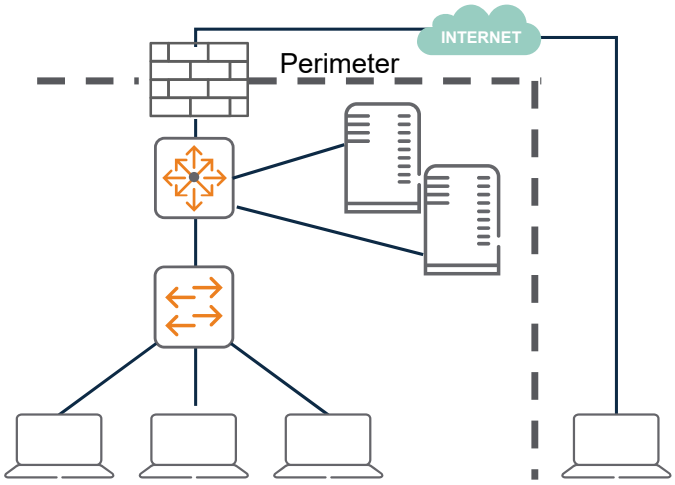
Internet of Things (IoT) devices, such as printers, cameras, smart thermostats, and many more, pose an increasingly critical vector for internal attacks. The number of these devices is growing exponentially. Global Workspace Analytics predicts that 55 billion IoT devices will be connected worldwide by 2022.

Because these devices often lack strong security, they represent billions of weak points by which hackers can gain internal access to a corporate network. An attacker with proximity to the corporate environment—perhaps from a lobby or parking lot—can try to access and compromise wireless-enabled IoT devices. If the perimeter firewall permits external management access to IoT devices, hackers could even attempt to log into the devices from the Internet using default credentials or common passwords. IDC found that only 5 minutes pass, on average, between the time an IoT device goes online and an attack is launched on that device.

Once hackers have compromised an IoT device, they can use that device as a backdoor for reaching other internal resources, exfiltrating data or launching other attacks.

Common Internal Threat Vectors

Remote Workers



- Increasingly common
  - 25-30% of workforce by 2021
- Outside of corporate firewall and exposed to malware
- Backdoor into the corporate network

MOD 1- 8

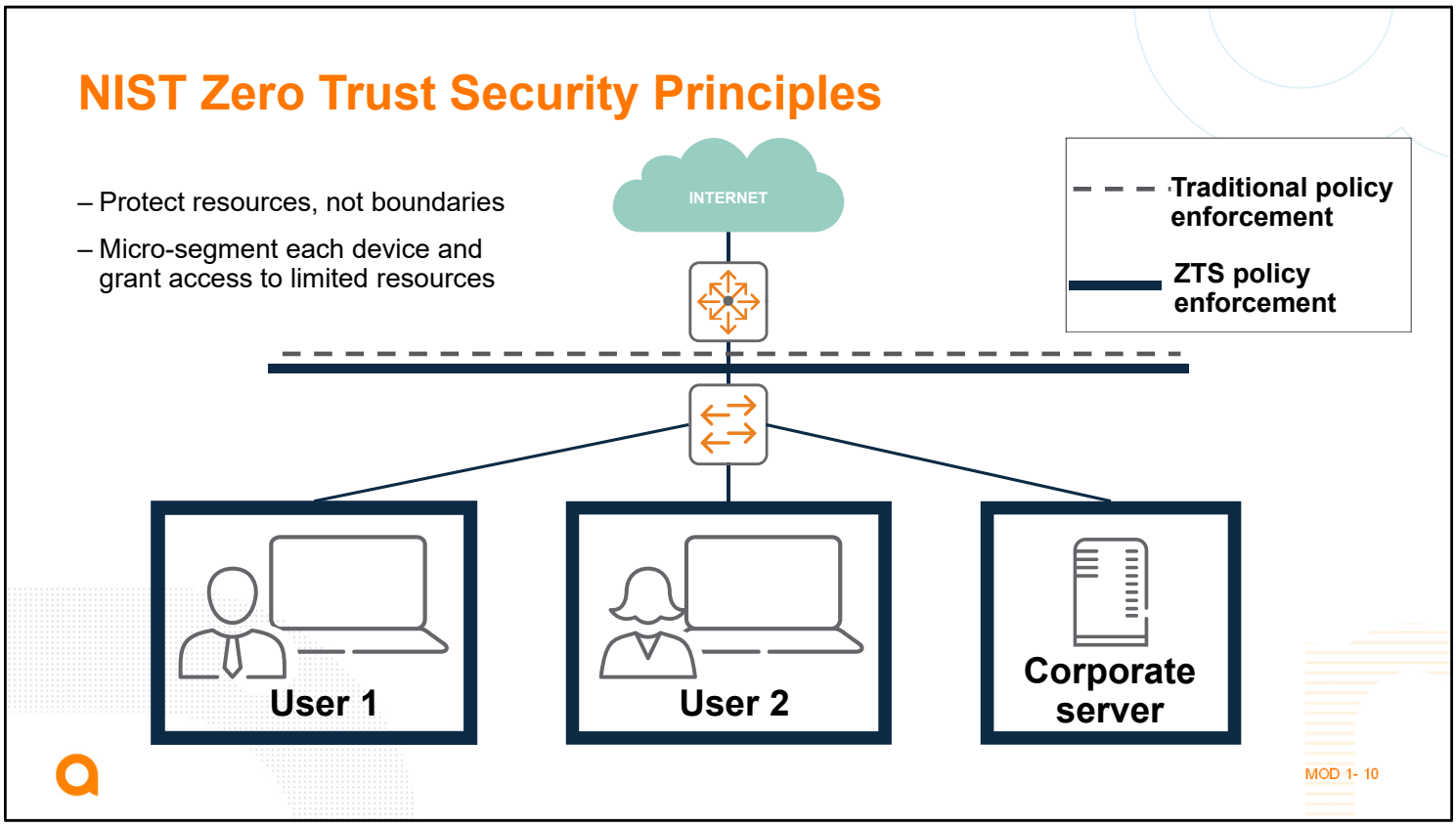
Remote workers pose another mechanism by which hackers can infiltrate corporate networks. Netscout predicts that 25 to 30% of the workforce will still be working from home by the end of 2021, even though life may be returning to the norms that were shattered by the pandemic. Because the workers are accessing the Internet from outside the safety of the corporate firewall, their devices might become compromised by malware that gives hackers a backdoor into that device. The hackers could then use the remote workers' access into the corporate network as a way to infiltrate the network.

What is Zero Trust Security?

Controlling and monitoring *all* devices regardless of location

These trends in threat vectors are dissolving the line between an external “untrusted” network and an internal “trusted” network. Companies need a security approach that acknowledges this reality: simply because a user or device is internal does not mean that the device can be trusted.

Zero Trust Security confronts this reality. It requires companies to treat all devices as inherently untrusted, regardless of their location outside or inside of the corporate network. By controlling internal devices and continuously monitoring them, the organization can limit the scope of damage that bad actor who gains internal access can do.



Zero Trust Security is an industry-wide trend, and several trusted sources have begun to define what it means. One of those trusted sources is the National Institute of Standards and Technology (NIST), a US agency that defines many security best practices. NIST is encouraging organizations to adopt a zero trust approach. Its zero trust architecture (ZTA) provides a broad framework in which many technologies can fit.

A key feature of the ZTA is a focus on protecting resources rather than protecting boundaries. When companies protect perimeters, a hacker who manages to get past the perimeter has an easier time invading systems, exfiltrating data, and attacking the company. And a perimeter-based approach cannot protect against the internal threat vectors you just examined. With ZTA, every client is tightly controlled, including internal ones. Policy enforcement and decision points identify each user and device on the network and grant that user or device only the level of access to resources required for that particular entity to do his, her, or its job. This approach is sometimes called micro-segmentation. Rather than control traffic as it passes from one large segment, such as the external network, to another large segment, such as the internal network, micro-segmentation controls all traffic between all devices, applying granular controls based on identity and device type.

For more information, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.

Forrester Zero Trust Security Principles

Enforce access control on all users and devices

Continuously monitor and analyze

MOD 1- 11

Forrester, a prominent industry analyst, is similarly guiding organizations towards a Zero Trust Security approach. Forrester emphasizes that in a Zero Trust Security network you do not trust any data, people, devices, or workloads absolutely. Instead you must monitor all users, devices, and applications and take appropriate steps to control how they use the network. In this effort, visibility, analytics, and orchestration across multiple security components will be key.

Forrester recommends that customers protect their network by identifying sensitive data that needs to be isolated and protected. To achieve this protection, the company should implement micro-segmentation by applying access controls to all clients. Remember: no users are absolutely trusted. Companies must define policies to dictate which authenticated users are allowed access to which data. And these policies must apply to users no matter how and where the users access the network, although customers might choose to use this contextual information to adjust the access policies to the situation.

Finally, Forrester recommends that customers continuously monitor and analyze the environment to discover threats and address security incidents in real-time.

(The information about Forrester's ZTN approach is taken from "Five Steps To A Zero Trust Network," Forrester, Stephanie Balaouras, Chase Cunningham, and Peter Cerrato, October 2018.)

Question #1

Zero Trust Security

Which correctly describes Zero Trust Security?

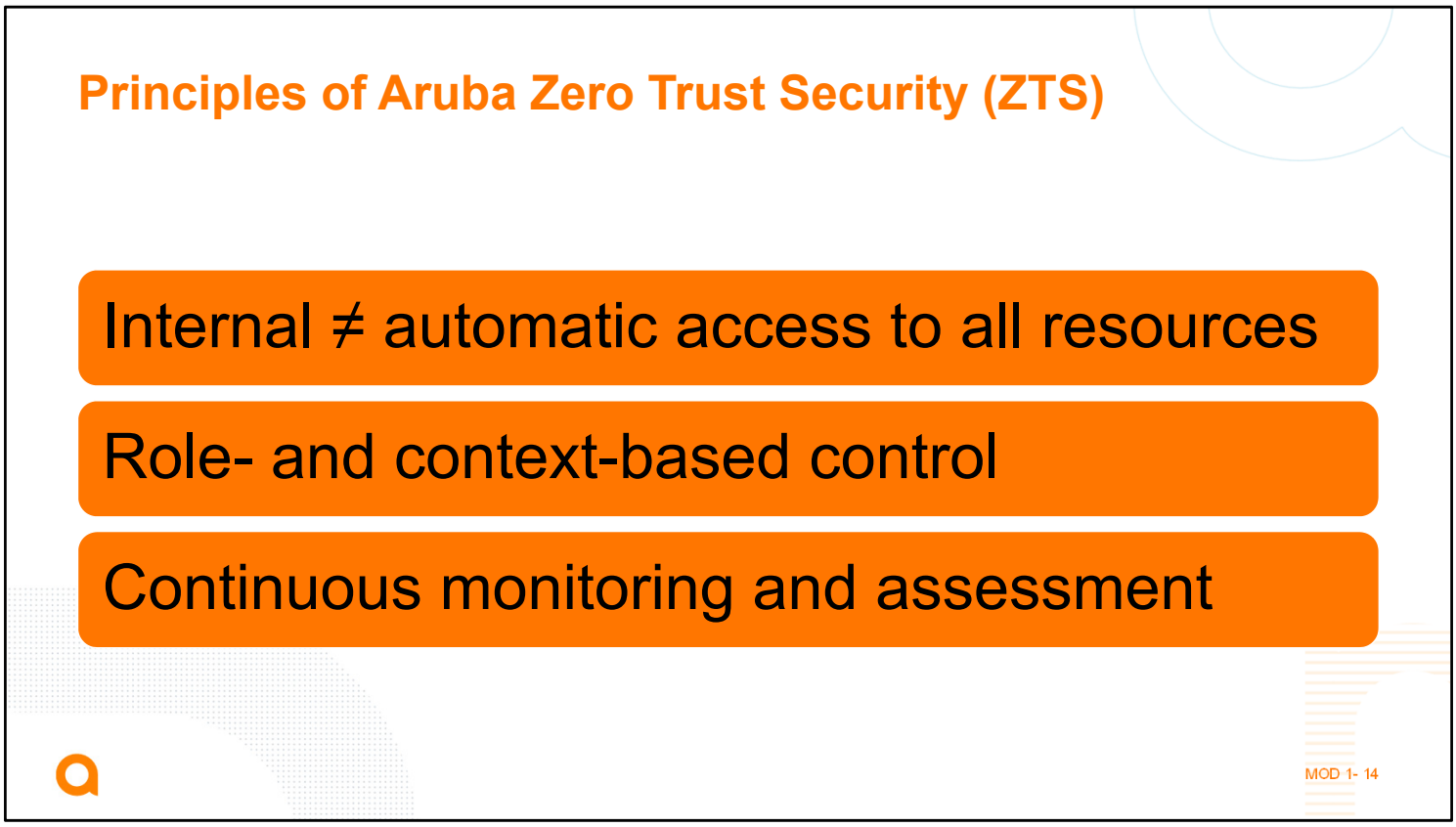
a. External clients are untrusted, while internal clients are trusted.
b. The perimeter is enhanced by a demilitarized zone (DMZ).
c. All users and devices are identified and controlled with granular, identity and context-based policies.
d. All users are considered equally untrustworthy and are given the same privileges regardless of identity.

Take a moment to review what you have learned so far about Zero Trust Security and the guiding principles behind this approach. Which correctly describes Zero Trust Security? Select one.

The answer is:

C. All users and devices are identified and controlled with granular, identity and context-based policies.

Topic 2: Aruba Zero Trust Security

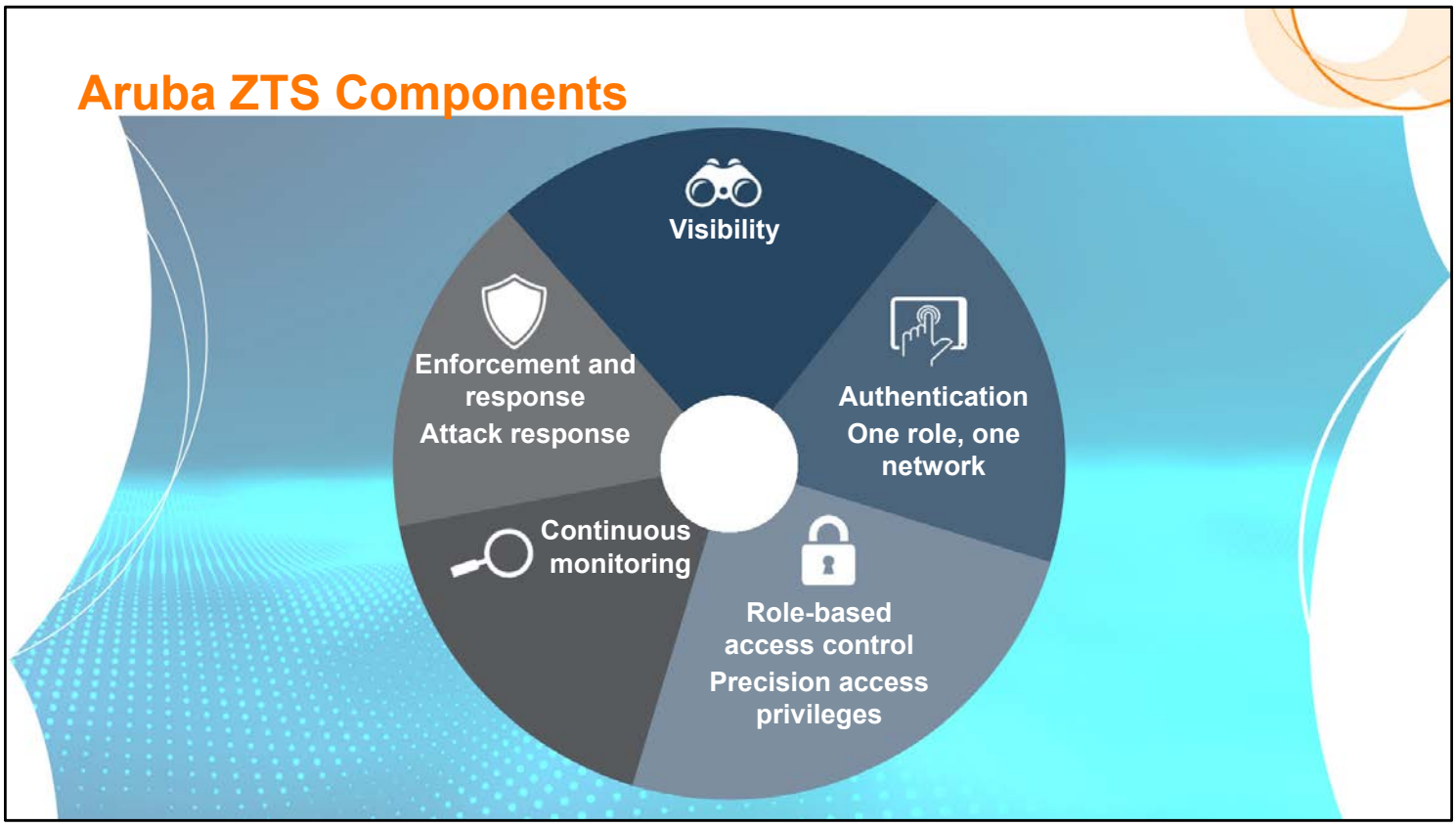


Aruba Edge Services Platform (ESP) includes Zero Trust Security (ZTS) as one of its key components. Aruba ZTS follows industry guidelines with three key principles: control over internal access, role- and context-based control, and continuous monitoring and assessment.

Default deny means that the Aruba network never grants a device access to resources simply because that device is internal. Instead the Aruba network uses authentication to determine who is connecting to the network and visibility to determine what is connecting to the network.

An Aruba network dynamically segments the traffic for every device that connects to it. This means that the network does not rely on static or location-based segments such as VLANs to determine how to control user traffic. Instead the network dynamically adapts to each device as that device connects, implementing role- and context-based access controls specific to the user role and device type. Aruba recommends a least access privilege approach, which means that users and devices are given access to as few resources as possible, while still enabling productivity.

Continuous monitoring and assessment entails an immediate response to threats, followed by recurring validation, so if a user is determined to be cleared from one security threat, their future access is not guaranteed without further monitoring.



Aruba takes a multi-faceted approach to security. Aruba ZTS solutions monitor and control every user and device that connects to the network, not just once, but continuously.

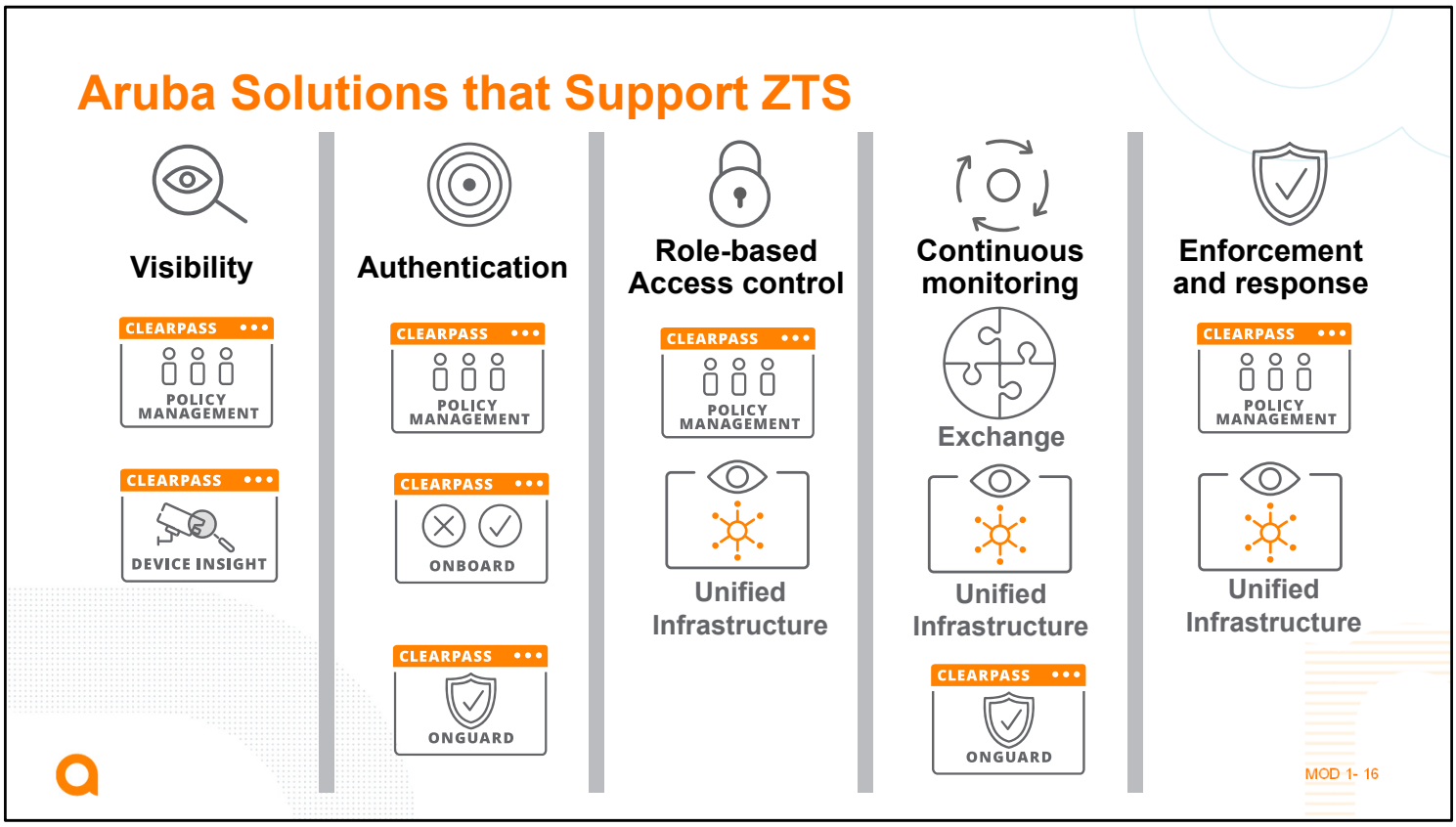
A broad range of authentication options, including both Authentication, Authorization, and Accounting (AAA) and non-AAA options, ensure that only authorized devices receive network access. With Aruba, a user's network experience is defined not by their location or access type, but by their role. Aruba's "one role, one network" approach means that users receive consistent and appropriate access rights based on their role, whether they are connected from a wired device at their desks, a wireless device in a conference room, or a remote device from home.

Role-based access controls power Aruba's approach. After authenticating every client and assigning it a role, the Aruba solutions enforce precise access privileges to micro-segment every client. While based on identity, these privileges also take context into account. For example, Aruba solutions can enforce different privileges for a user on a laptop and for the same user on a smartphone, in keeping with the different security profiles of those devices.

Because Aruba understands that a ZTS solution can never authorize a client and then forget about it, connected devices are continuously monitored. Aruba solutions collect real-time telemetry information to detect intrusions and other threats. They also monitor a broad range of clients, traffic, and behaviors because not only do our Aruba solutions have embedded capabilities, but they also integrate with more than 150 third-party products.

Every threat detected through monitoring requires a response. Aruba solutions make those responses faster and more powerful. When a triggering event occurs, such as the detection of a malware-infected device, our solutions can take a variety actions, including locking an infected device out of the network or placing it in a quarantine segment for remediation.

Finally, because you can only secure something if you know it's there and understand what it is, Aruba grants customers a high level of insight into the devices in their environment. Aruba solutions discover and profile all of the devices connected to a network. Advanced, custom fingerprinting technologies identify the precise type and operating system of each client.



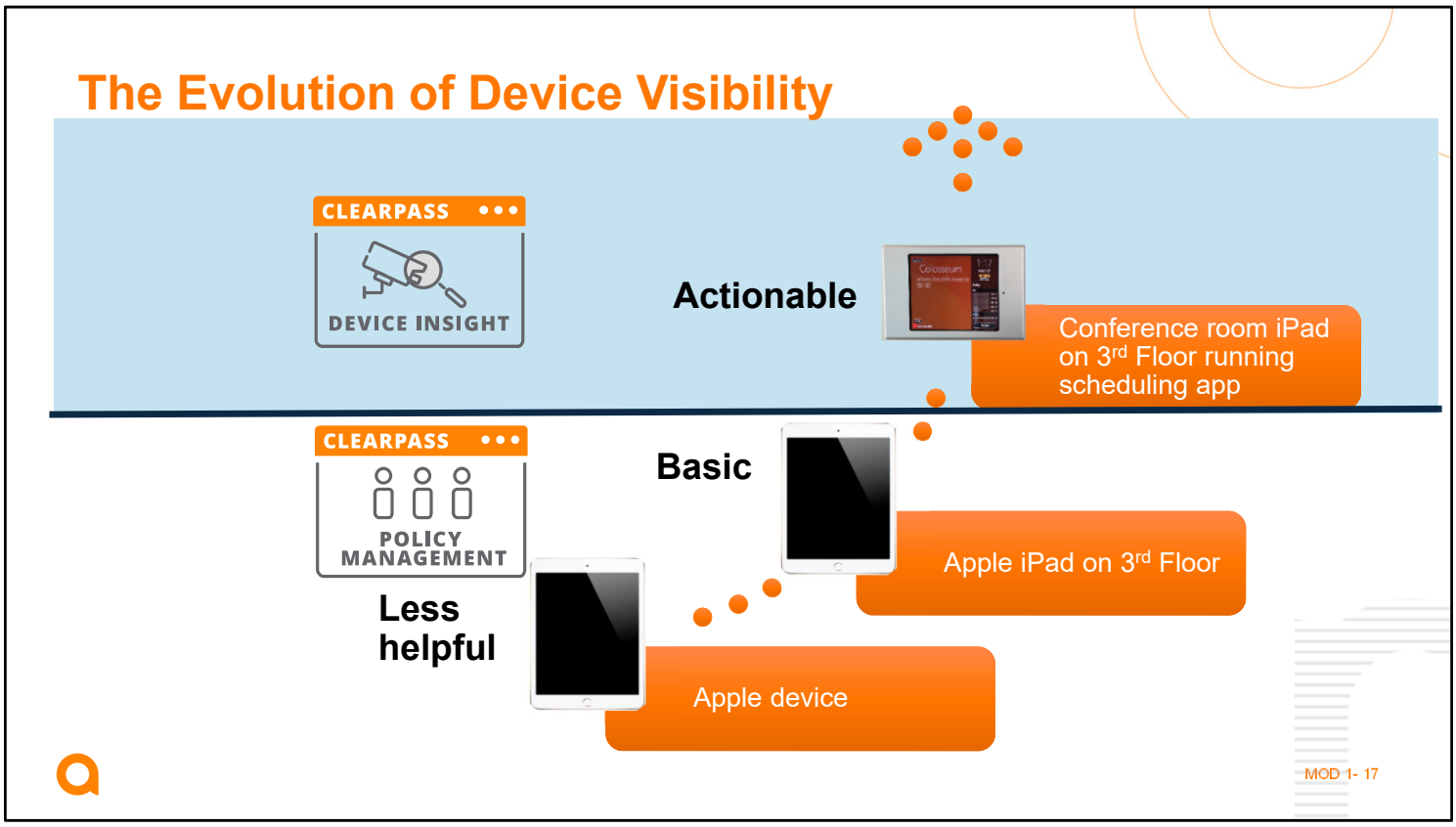
Here you can see which Aruba solutions support which pieces of ZTS. ClearPass Policy Manager (CPPM) provides some visibility benefits, while ClearPass Device Insight (CPDI) provides complete visibility for all of a company's heterogenous network.

CPPM provides a broad range of sophisticated authentication methods, and it is supported by ClearPass Onboard and ClearPass OnGuard. Building on its authentication capabilities, CPPM delivers role- and context-based access control based on highly flexible policies. The Aruba Unified Infrastructure receives the instructions from CPPM and enforces them with a powerful firewall.

The Unified Infrastructure also helps to deliver continuous monitoring. And companies can extend monitoring with a broad range of third-party solutions that are part of ClearPass Exchange.

Based on monitoring results, CPPM can make new decisions to respond to threats, and the Unified Infrastructure can enforce those decisions and mitigate threats.

Over the next several slides, you will dive deeper into how exactly each of these products help businesses achieve ZTS.

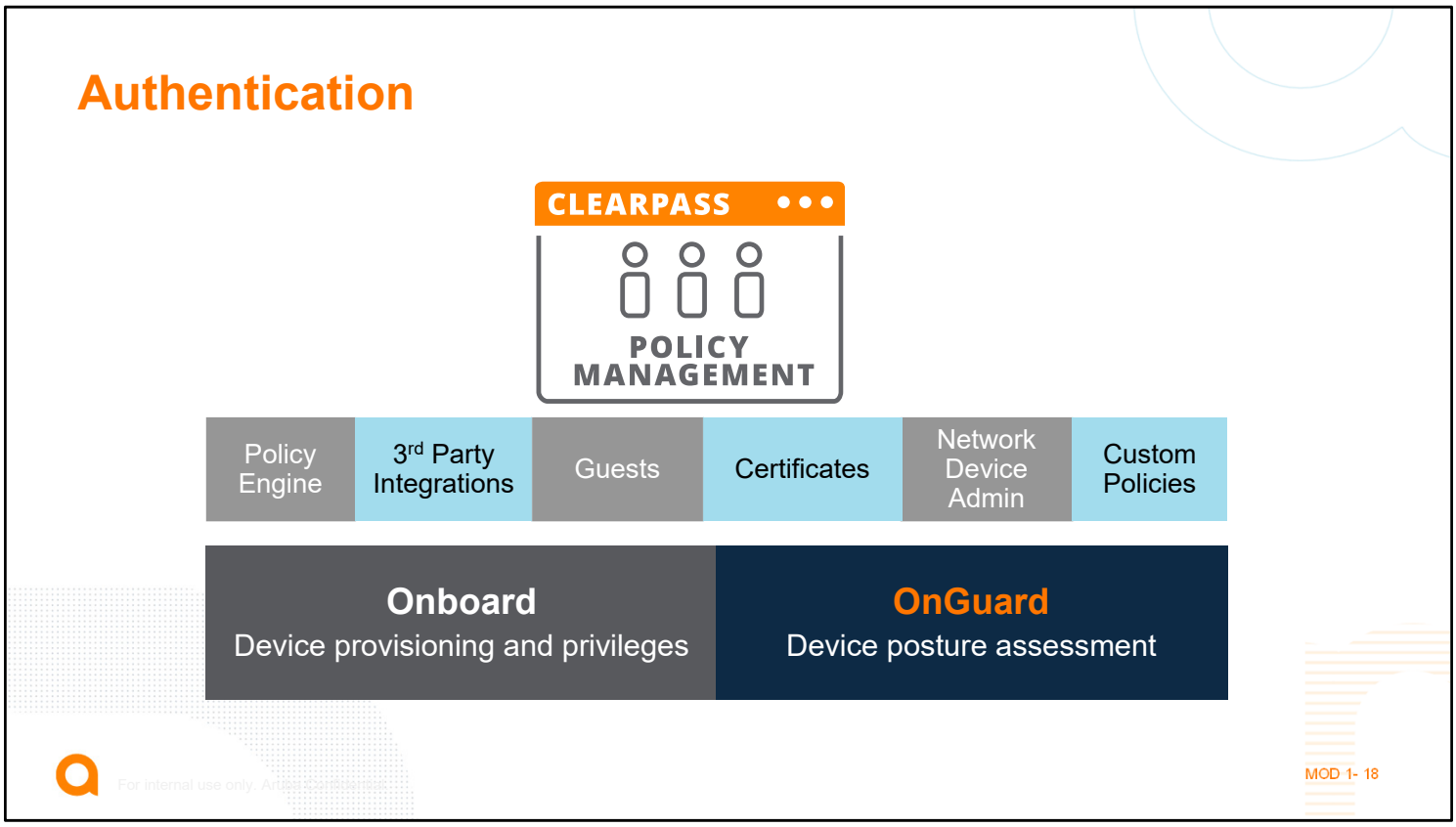


Good security begins with visibility—since security is only as good as the information it's based on.

Visibility has naturally evolved as time has passed, but you may find that some customers are still relying on antiquated visibility. This level of visibility is simplistic and unhelpful. It is often based on MAC address and DHCP. It might, for example, only inform you that an Apple iPad has joined the network. With the rising sophistication of exploits, this level of visibility is simply not enough.

Going one step up, many customers are still utilizing only basic visibility. This class of visibility includes solutions like SNMP, and is based on scans of the network. It offers more specific information about a device. For example, you might see that an Apple iPad has joined the network on the 3rd floor. CPPM provides this level of basic device visibility.

With ClearPass Device Insight, Aruba leads customers to actionable visibility. This level of visibility is based on the behavior of a client, and provides granular insights about each device on the network. For example, you would see that an Apple iPad has joined the network in the conference room on the 3rd floor and is now running a scheduling app. Actionable visibility provides the kind of detailed information that organizations need to protect themselves from today's attacks.

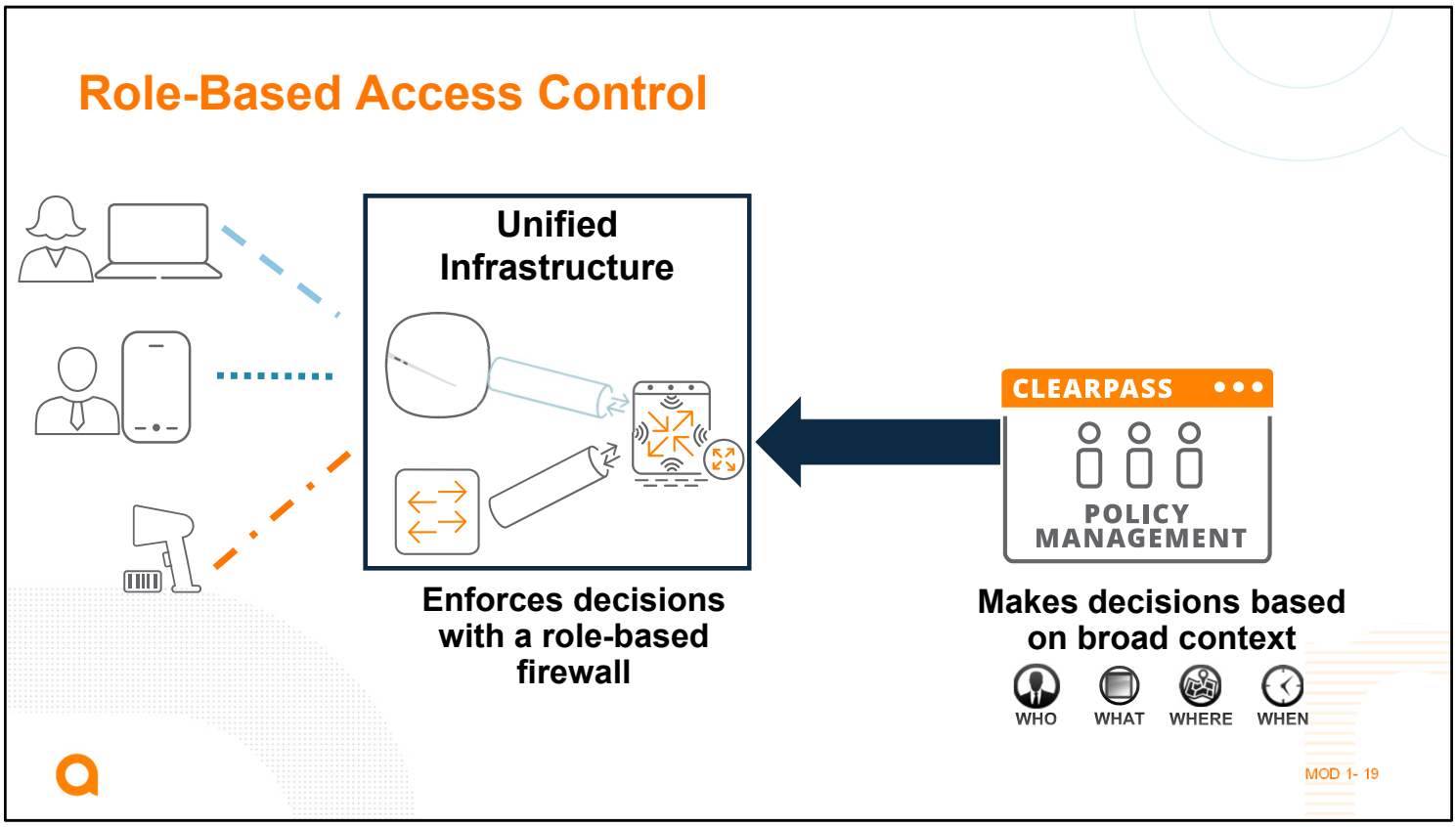


ClearPass Policy Manager (CPPM) acts as the central policy engine for controlling all forms of access. It supports multiple authentication methods, including integration with Microsoft Active Directory, a portal for guests, certificate authentication, and multi-factor authentication. CPPM allows network device admins to define custom policies based on a user's identity or device type. It also enables them to define policies based on context, such as a user's location or the time of day. And CPPM integrates with third-party solutions to enhance security orchestration.

Authentication with CPPM can be enhanced with ClearPass Onboard and OnGuard.

ClearPass Onboard simplifies the process of provisioning devices with the settings and certificates required for a secure authentication. Onboard provides a self-service app that enables users to provision their own devices, rather than making this another task for IT.

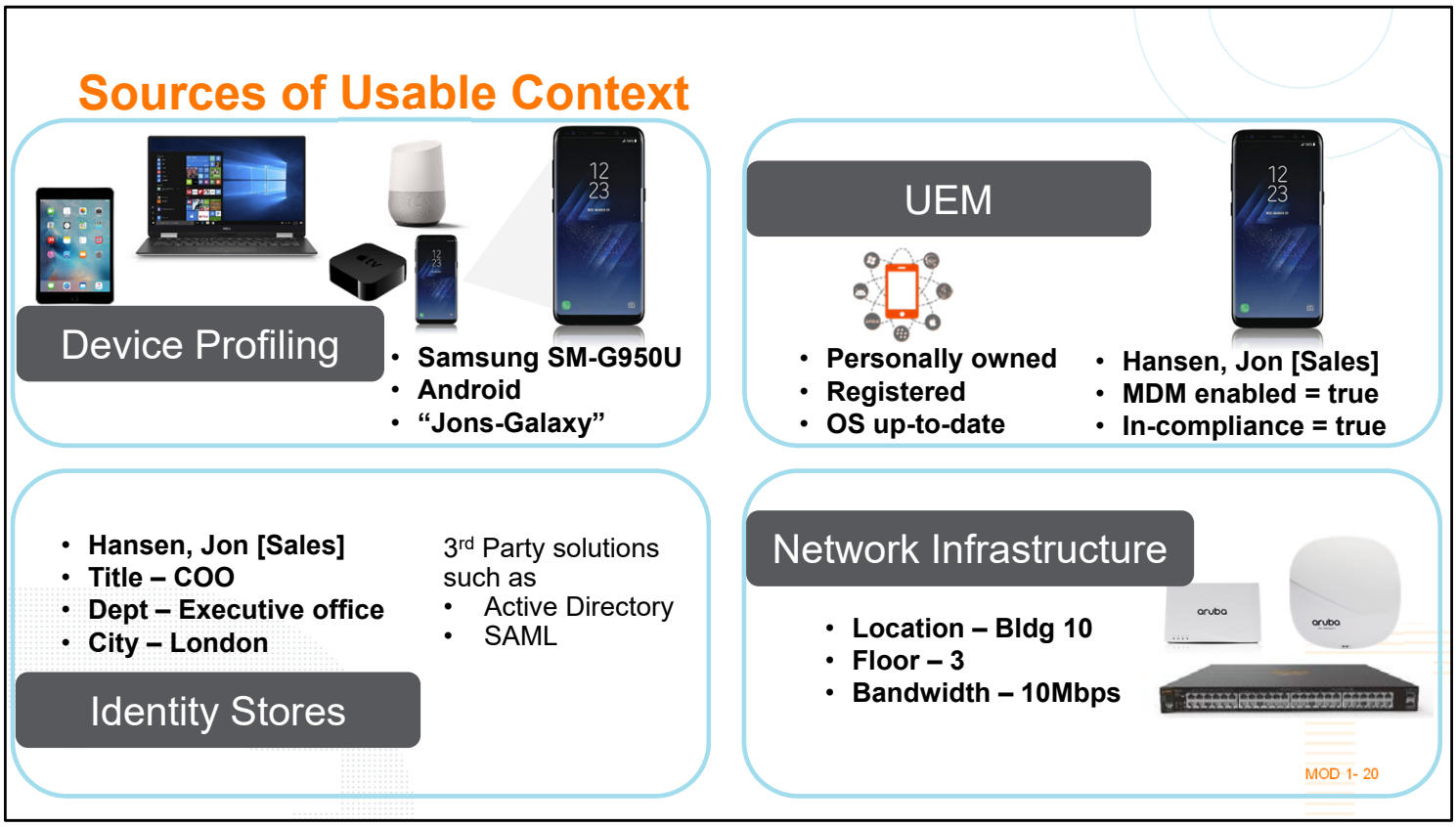
ClearPass OnGuard scans endpoints to determine their security posture. For example, it can verify firewall settings and ensure that a device's patches are up-to-date. OnGuard communicates information about an endpoint's security posture to CPPM. CPPM can then use that information to affect its access control decisions, deciding, for example, whether to quarantine the device.



To implement role-based access control, customers rely on Aruba infrastructure to take action based on the roles that Aruba CPPM assigns. Aruba APs and gateways provide a role-based Policy Enforcement Firewall (PEF), which filters all devices' traffic based on the CPPM-assigned role. For example, the PEF might allow a user with the HR role to access a subnet of servers that hold academic records while preventing other users on the same network from such access. The PEF might further restrict IoT devices to sending and receiving traffic from a very limited set of IP addresses.

Additionally, switches can tunnel clients' traffic to gateways, meaning that no matter what connection method users choose, wireless or wired, the same role-based policies will be applied to them.

An Aruba network can furthermore implement context-aware policies, which allows for the application of different policies to the same user, depending on the user's device. A user on a personal, insecure smartphone can be restricted from accessing certain corporate resources that the user can otherwise access on a company-issued laptop.

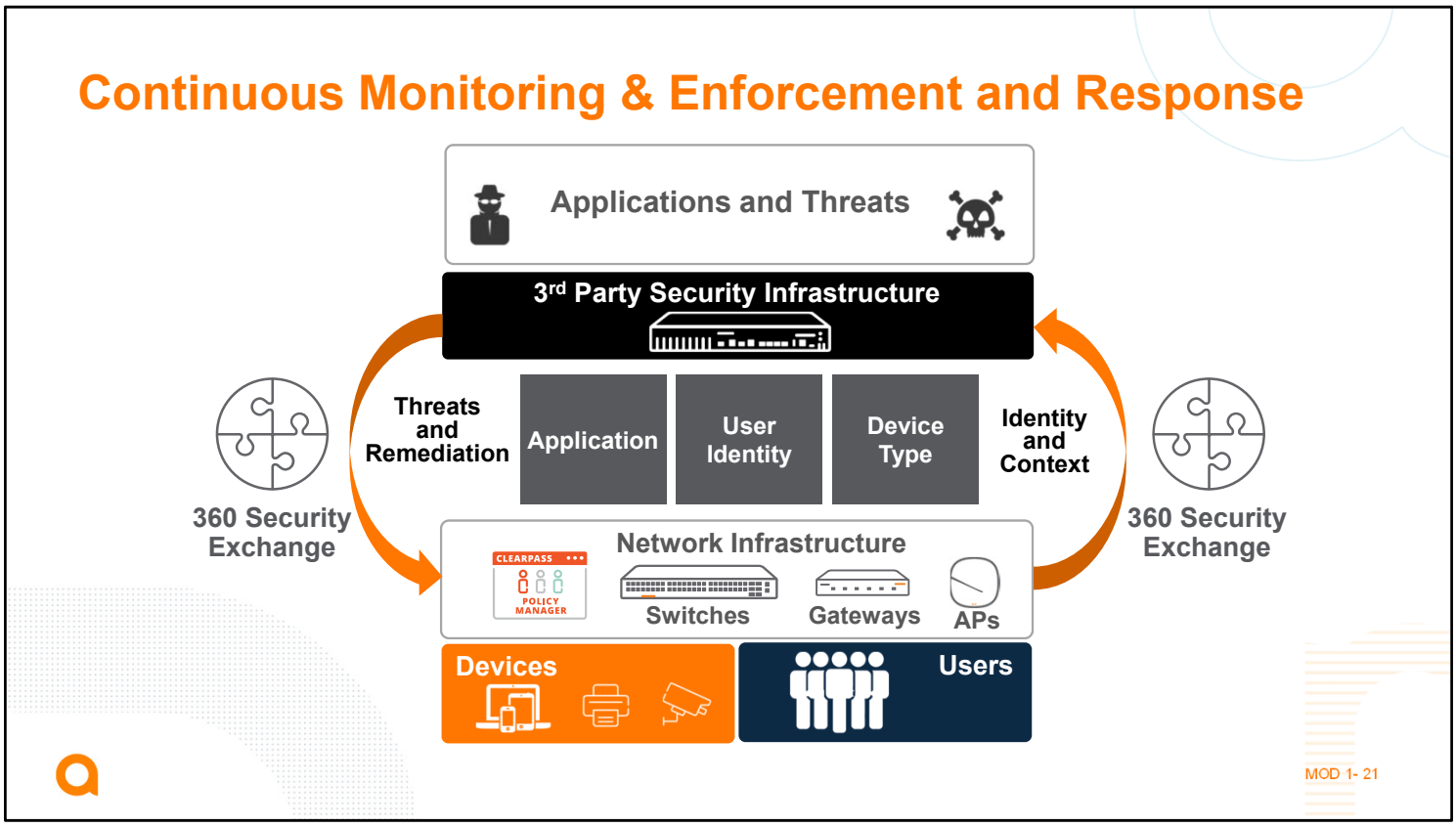


CPPM has several sources of information on which to draw for "context" for its policies. First, CPPM gains information from the devices themselves. CPPM can implement device profiling, or it can integrate with CPDI for more advanced profiling. Device profiling yields information such as the device OS and category. For example, Aruba solutions can distinguish between a laptop and a smartphone, and it can determine the hardware vendor for the smartphone. As you learned, CPDI distinguishes itself in the depth of visibility that it provides for IoT devices. Using this information, CPPM can assign a role with less trust to more vulnerable devices, helping to prevent these devices from becoming backdoors for attackers.

CPPM can also integrate with unified endpoint management (UEM) tools to gather context. With this data, CPPM can determine if a device's OS is up-to-date or if the device is overall in-compliance. If the OS is not up-to-date or the device is not in-compliance, the Aruba network can react accordingly to protect the network from this vulnerability.

CPPM also uses identity stores to obtain more user-centric context. For example, the name, title, department, and location of an employee will be available through sources like Active Directory, which allows CPPM to precisely limit users' access based on their actual needs.

Finally, CPPM can also obtain contextual information from network infrastructure devices. Based on information included by the network access device (NAD) in its RADIUS request, CPPM can determine the client's location and apply location-based policies. It can also use accounting information from NADs to track clients' bandwidth consumption.



The last two elements of Aruba's Zero Trust Security approach are closely related.

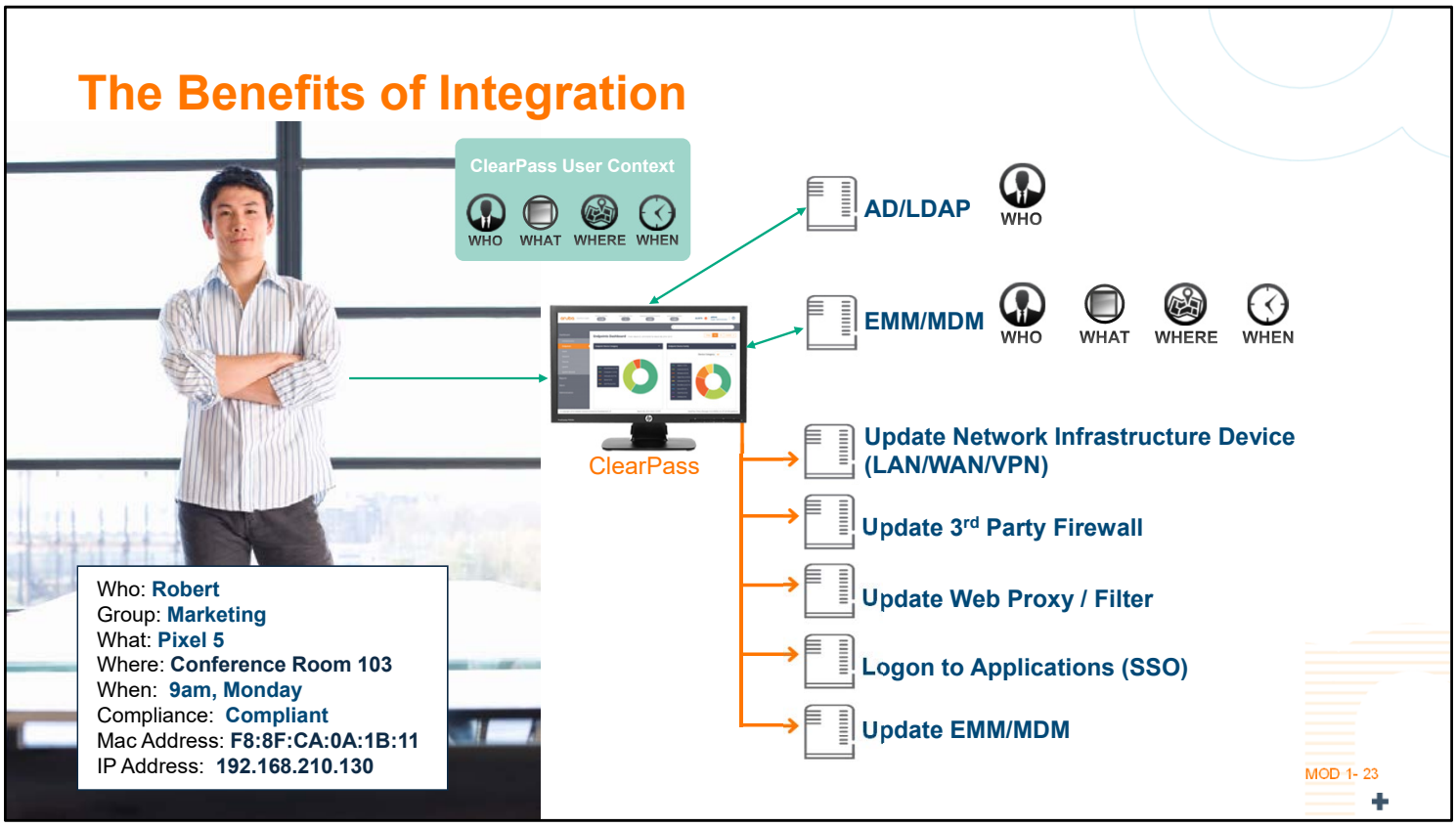
Aruba infrastructure conducts continuous monitoring on all connected endpoints to ensure that they are behaving appropriately. Built-in functionality such as intrusion detection, deep packet inspection (DPI), and web-traffic filtering based on site reputation make this possible. Aruba solutions also integrate with more than one hundred and fifty third-party solutions in the Aruba 360 Security Exchange.

Through 360 Security Exchange, Aruba can feed third-party tools important contextual information such as user identity and device category. In return, those third-party solutions can detect endpoints that are infected with malware, identify the source of an attack, and so on, before subsequently remediating the threat.

Finally, Aruba supports enforcement and response primarily by adjusting an endpoint's access level. For example, if CPPM receives information indicating that an endpoint has been infected with Malware, Aruba solutions will lock out that endpoint, or place it in quarantine and direct the user's browser to a remediation server.

Here you see just some of the many third-party solutions that can integrate with CPPM. These solutions span many categories, including security and authentication. Companies can even choose to let guests login with credentials from popular social media platforms.

By integrating with logging solutions, CPPM helps to create audit trails and support companies' organization-wide security efforts. Integration with Enterprise Mobility Management (EMM) solutions can help to provide important context, as you learned earlier, and CPPM integrates with many commonly used ones.

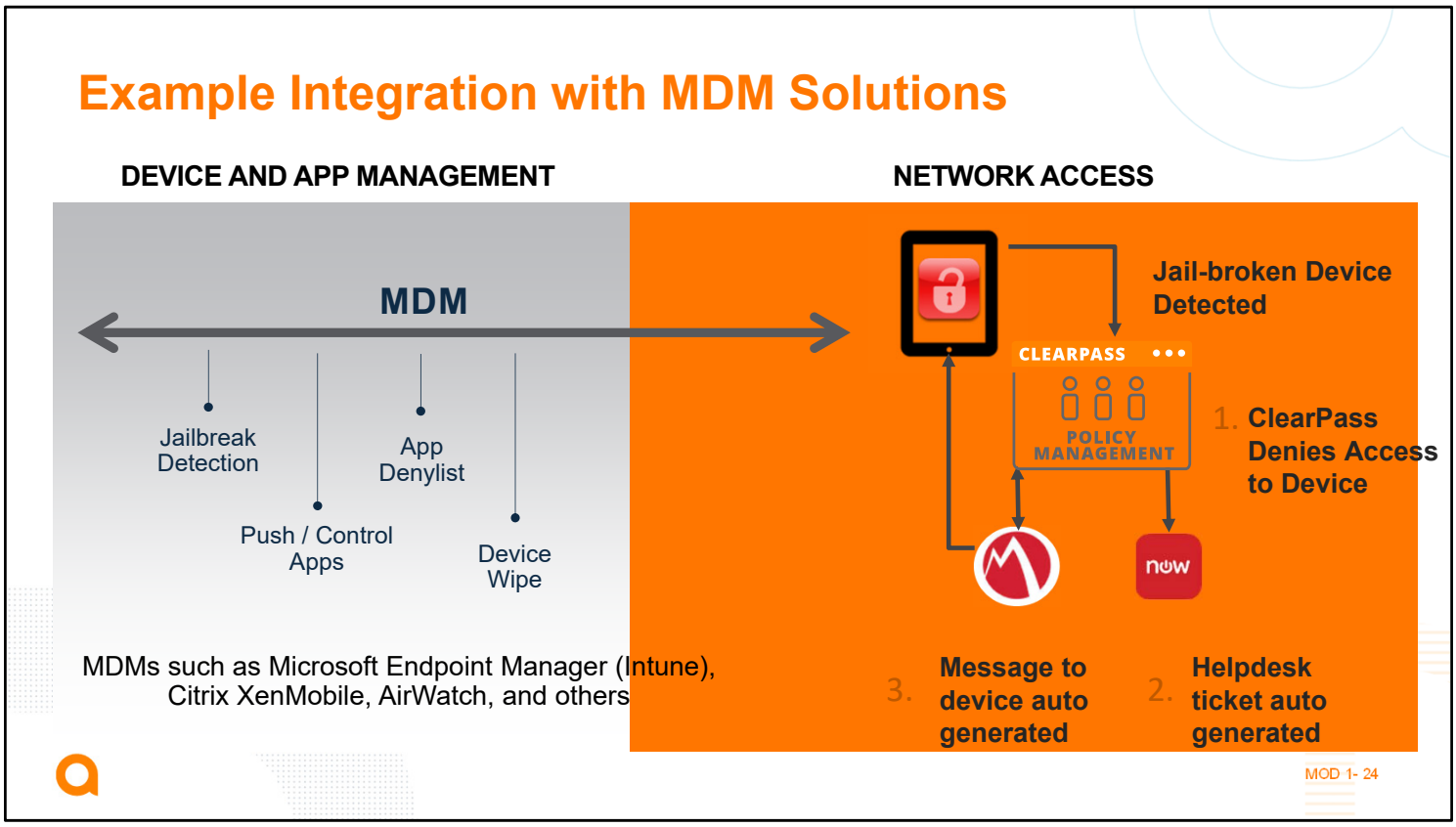


By integrating with third-party solutions, CPPM is able to assign policies with much greater accuracy based on who the user is, what device is in use, where the client is located, and the time at which they are trying to access network resources.

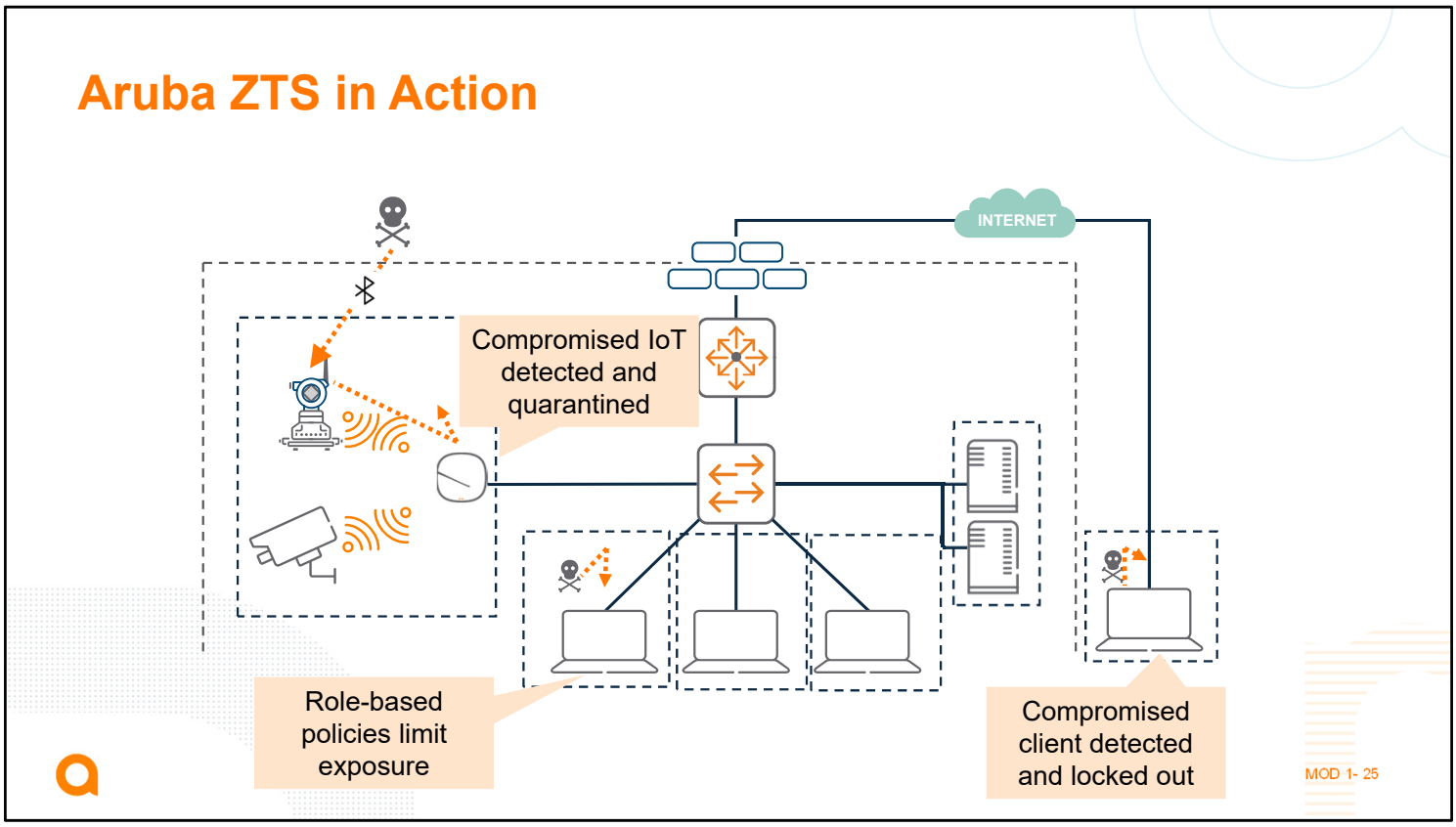
With third-party integrations, CPPM is able to derive users' identity primarily from apps that users regularly interact with, like Active Directory. CPPM relies on other third-party solutions, especially mobility management solutions, and its integrations with them to further derive user identity, and all the other relevant information about that client.

Consider a company that is using AD for its directory service and MobileIron MDM for security and management. CPPM can utilize integrations with these solutions to build a profile of the user, who, for example, tries to access files stored on a corporate server using a mobile device. Rather than being an anonymous user on a mobile device, CPPM now identifies this user as Robert from Marketing, using his Pixel 3 in Conference Room 103 at 9 AM on Monday morning to access corporate resources. The device is determined to be compliant with security policies. Its MAC and IP address are naturally known as well.

Now, CPPM can update enforcement devices, the firewall, and the web proxy with policies that are appropriate for Robert. CPPM can adjust Robert's ability to logon to applications, and even update MobileIron to ensure Robert and his device are still secured effectively.



As another example of strengthening security with third-party integration, consider what might happen if a jailbroken device joins the network. A mobile device management (MDM) solution would be capable of recognizing that the device is jailbroken—and represents a security threat to an enterprise environment. Through integration, CPPM could then be alerted about the jailbroken device, and subsequently determine that access should be denied. A helpdesk ticket would be autogenerated by CPPM. And CPPM can request the MDM solution to notify the user why they did not receive a connection, and what action the user can take.

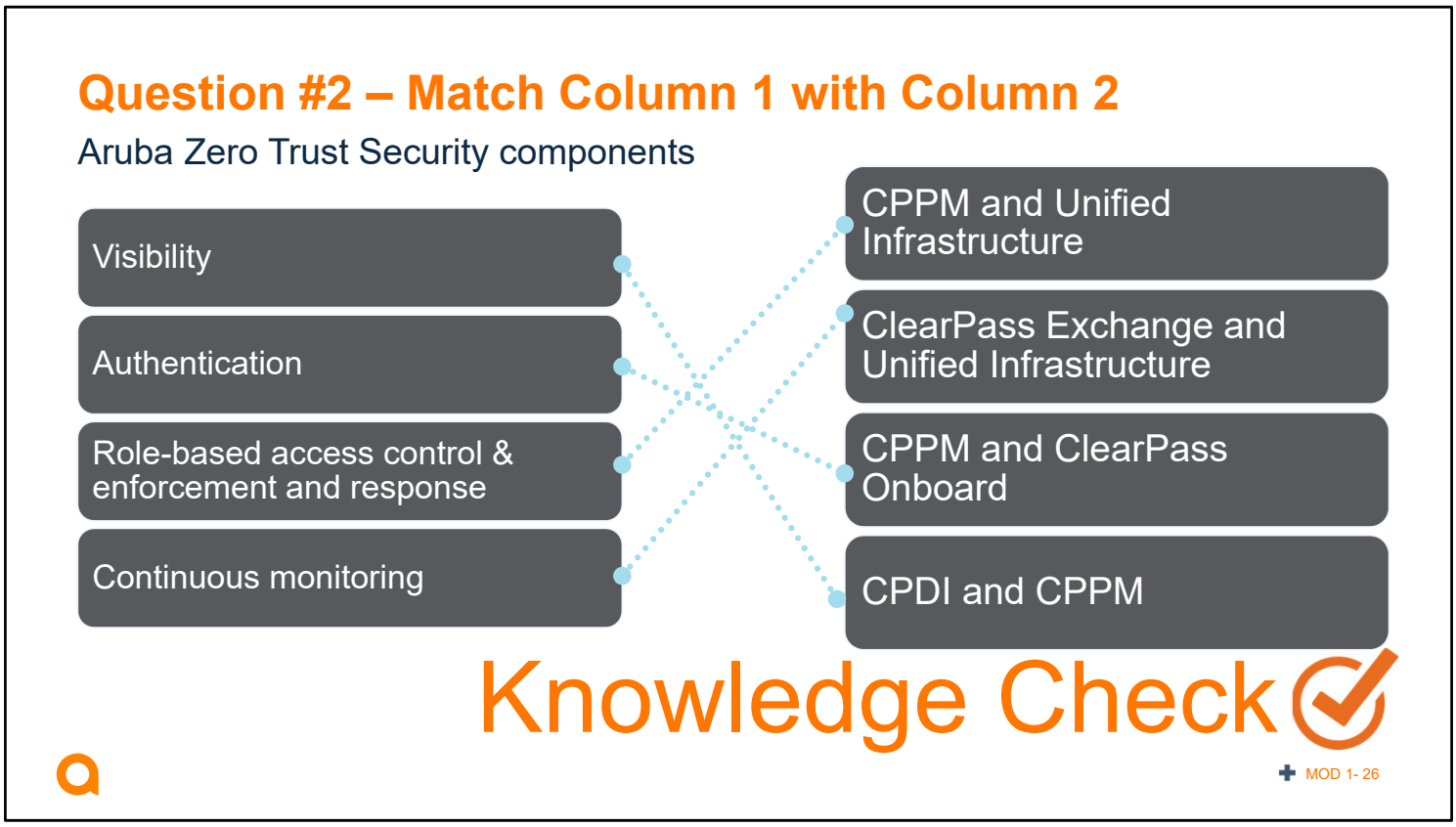


Now look at some more examples of how an Aruba ZTS can secure a network against internal threat vectors.

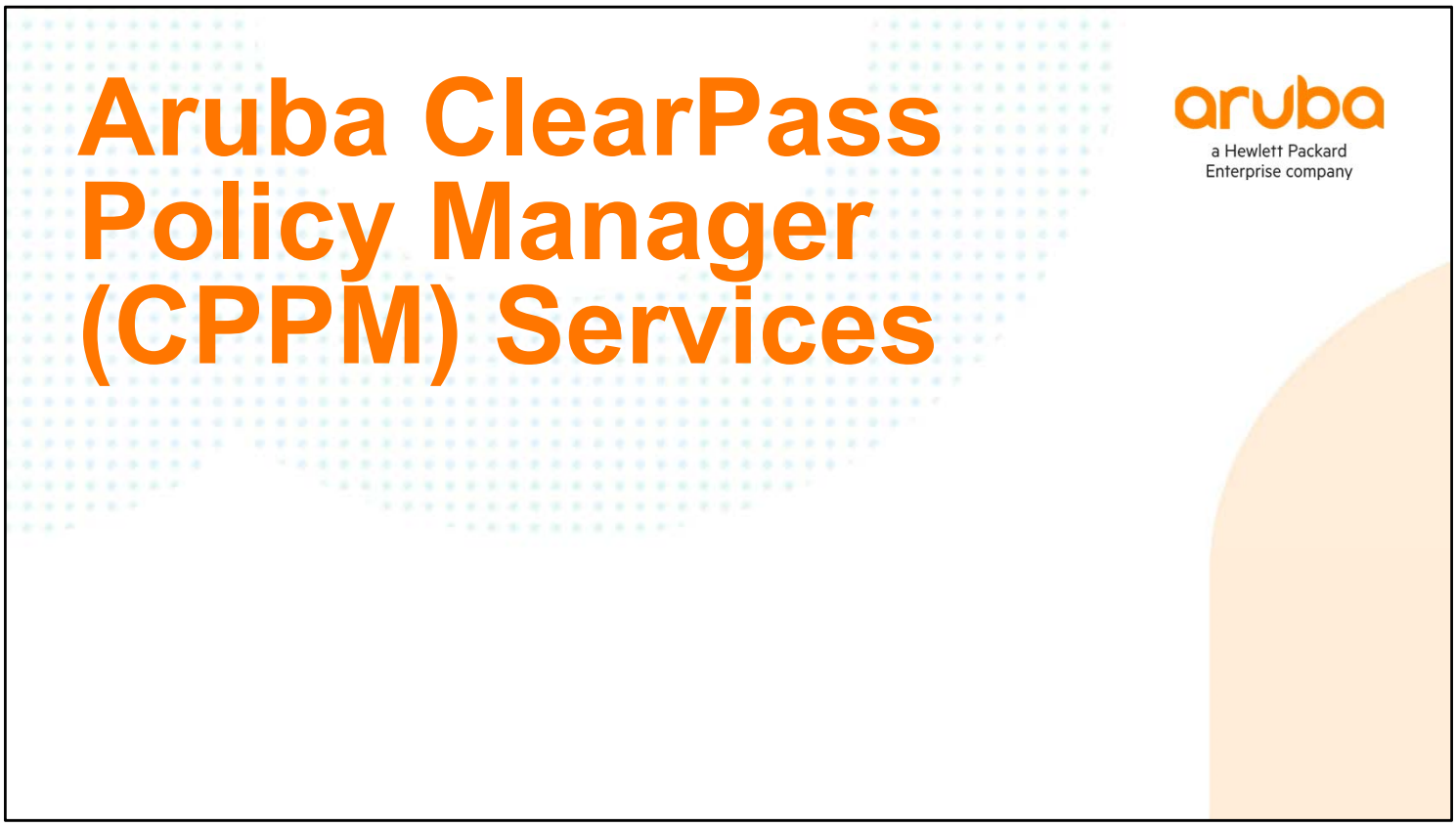
Perhaps hackers succeed in compromising an IoT device. Because Aruba ZTS enabled the company to tightly control the types of traffic that IoT devices can send, the hackers will find it much more difficult to use the devices to reach sensitive resources. Similarly, perhaps a bad actor uses phishing and social engineering to install malware on an employee's device and covertly take control of that device. However, role-based access controls have denied this user from using SSH and also limits which data center networks the user can access. Again, the hacker is limited in ability to expand the attack to other devices in the system.

And by continuously monitoring internal devices, Aruba ZTS can detect suspicious behavior such as an IoT device that suddenly begins trying to establish SSH sessions with a broad range of IP addresses. The network can then take action to lock out the device behaving suspiciously.

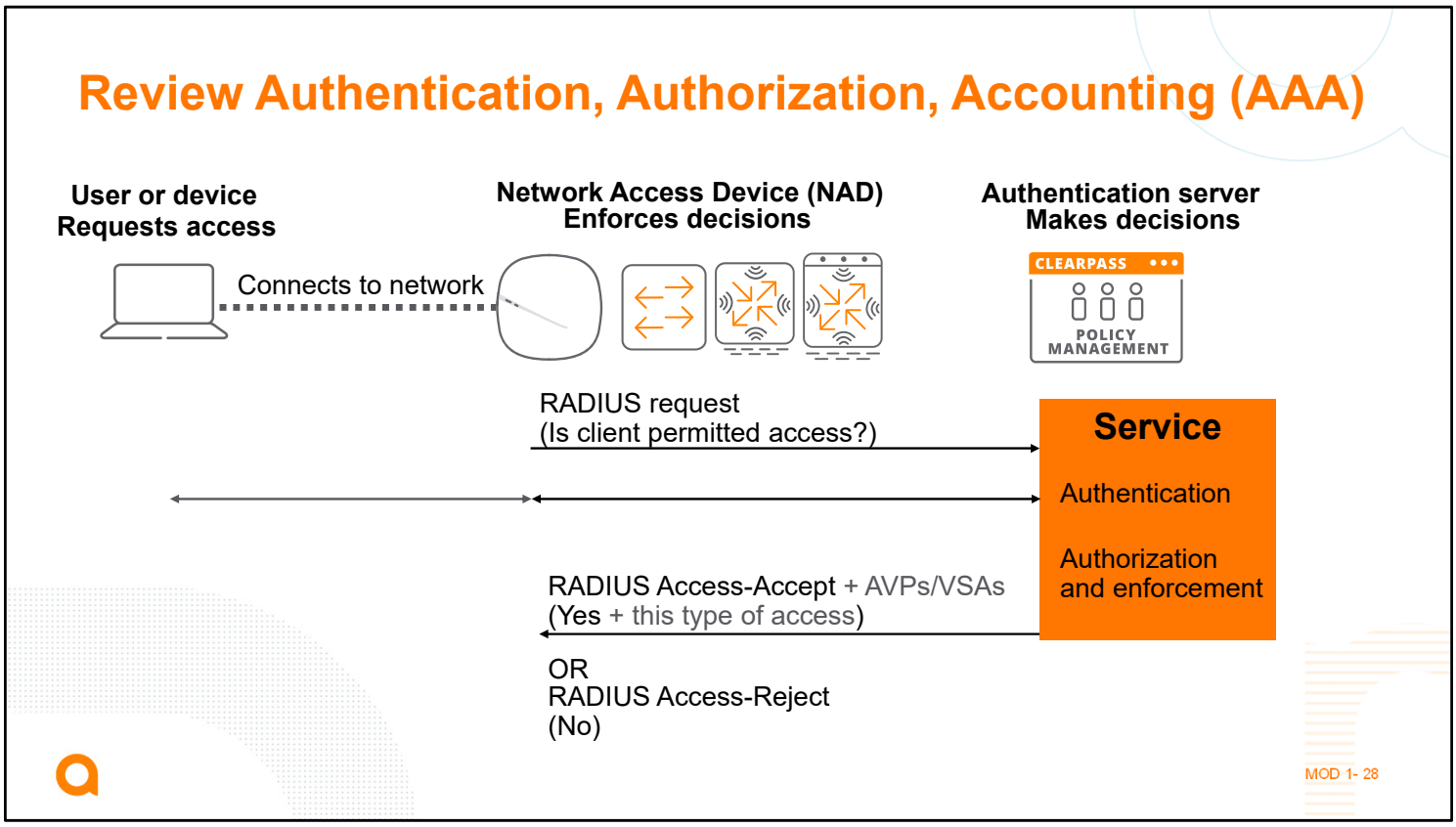
This is the substance of Zero Trust Security. The network never lets a device in and then forgets about it. By restricting each device to the lowest level of appropriate resources, and continually monitoring whether devices continue to merit that access, ZTS minimizes real damage to the network.



Take a moment to review what you have learned so far about Aruba's approach to Zero Trust Security. Match the Aruba Zero Trust Security principles to the products that allow customers to act on those principles.



Topic 3: Aruba ClearPass Policy Manager (CPPM) Services



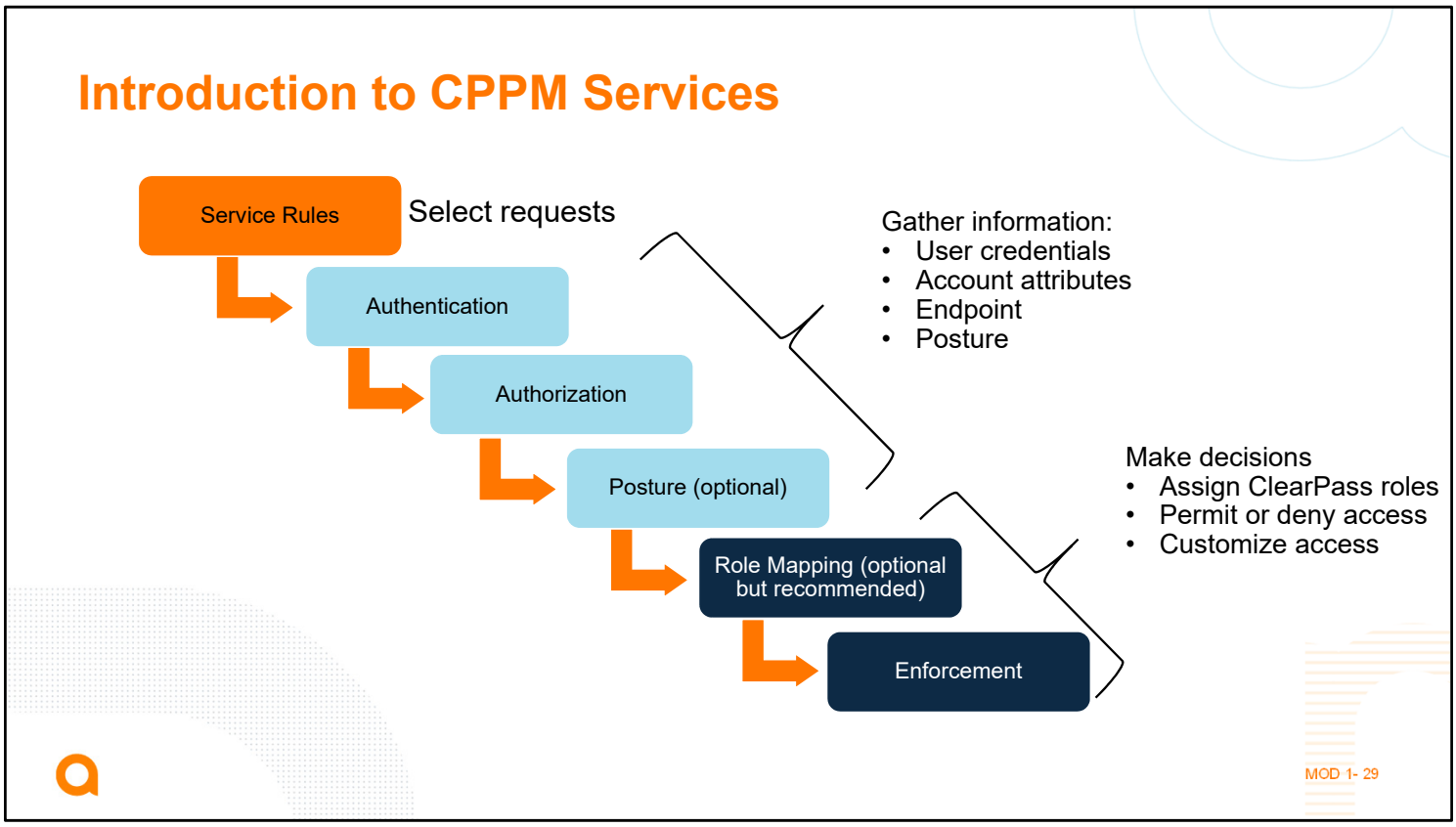
CPPM provides the foundation for Aruba Zero Trust Security, so you will now learn some fundamental concepts that will help you use this powerful tool to secure company's networks.

Among other capabilities, CPPM acts as an authentication server within the Authentication, Authorization, Accounting (AAA) framework. RADIUS is a common AAA protocol, and the one on which you will focus for the first part of this course.

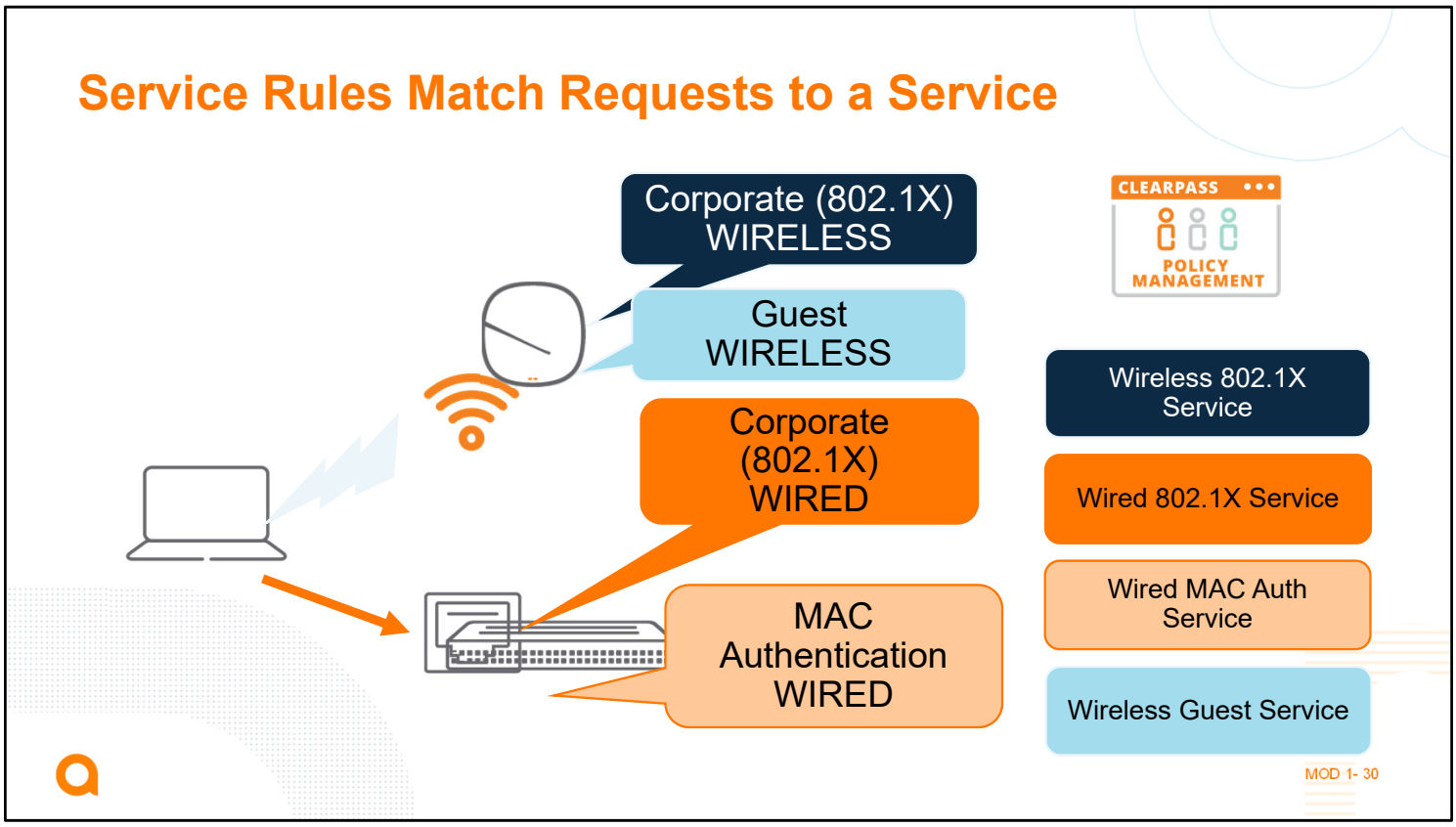
In AAA, a user or device—often called a client—requests access to a service. The client can request any service, but most often in this course, the client is requesting network access by connecting to the network. In that case, the AP, switch, gateway, or mobility controller (MC) to which the client connects is the Network Access Device (NAD). (In some cases, the NAD is referred to as the Network Access Server (NAS). The NAD sends a RADIUS request to its authentication server to ask whether the client is permitted access.

As authentication server, CPPM must first authenticate that the client is who and what it claims to be and, second, authorize the client for the correct level of access. It matches the RADIUS request to a service and uses that service to process the request. First, it implements the authentication method listed in the service. Often that method calls for CPPM to exchange several more RADIUS messages with the NAD. If the NAD is enforcing 802.1X, the NAD actually acts as a go-between for the client and CPPM, which exchange Extensible Authentication Protocol (EAP) messages.

As an end result of these communications, the client has passed or failed authentication. The CPPM service further processes the request and determines whether an authenticated client is allowed access and at what level. If CPPM decides the client is allowed, it sends the NAD a RADIUS Access-Accept. This message often includes attribute value pairs (AVPs) or vendor specific attributes (VSAs), which further define the level of access. If CPPM determines that the client is not authorized, it sends a RADIUS Access-Reject.

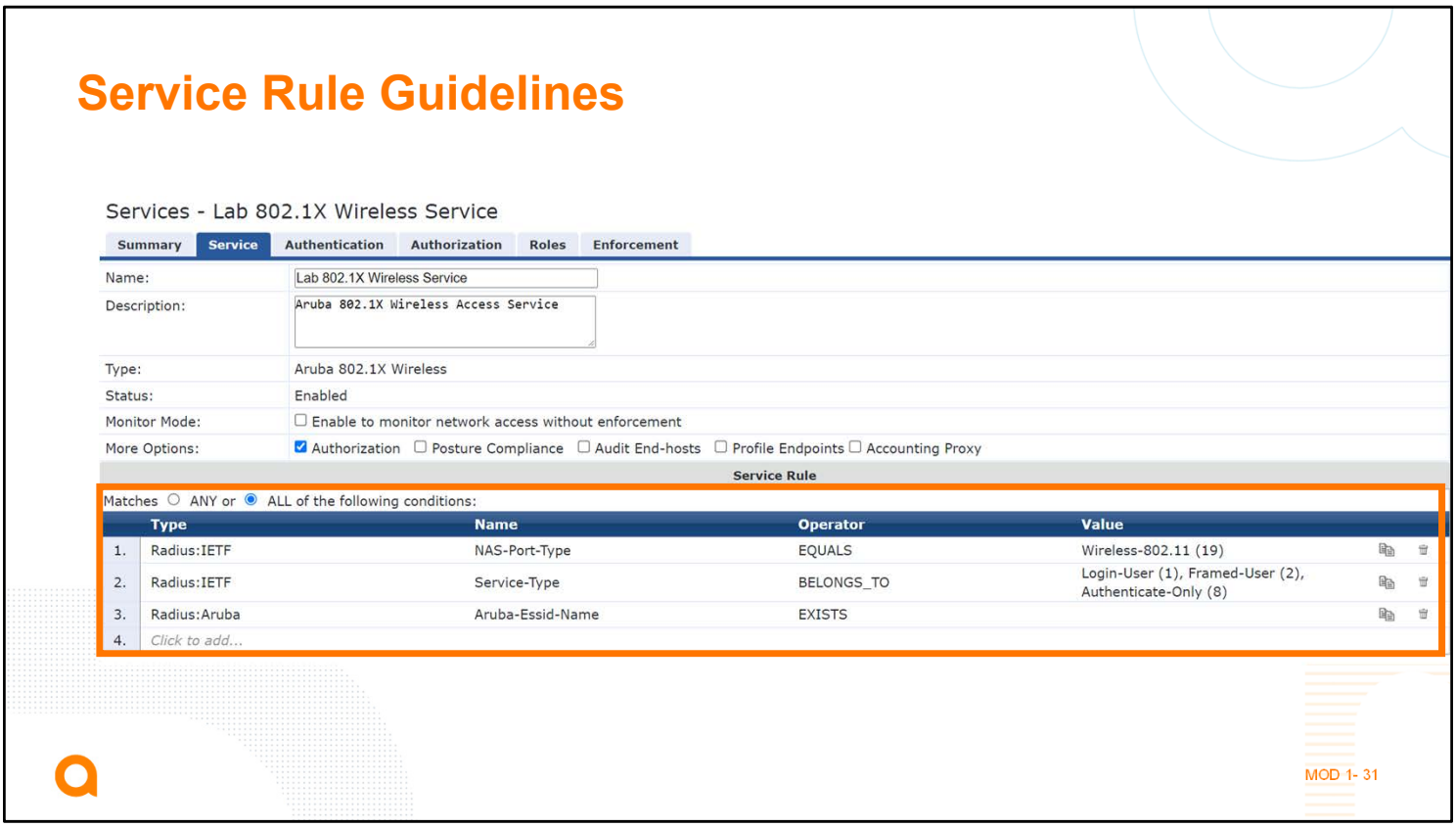


When CPPM processes a request it follows a set pattern. Starting with service selection, CPPM matches the request to the proper service. Then CPPM gathers information about the request such as the users credentials, account attributes, endpoint profile context, or the client's health status and the source and type of request. The service also gathers profile information about the device making the request. Finally, with all of the data collected, the service roles mapping and enforcement processes can make decisions and reply to the request. The service implements the organization's desired access policies by evaluating the data collected and matching it to rules built in the enforcement policies. Services are custom built to support various scenarios that the organization wants to support. In this way CPPM has the ability to process a large number of different requests from different networks.



The service selection rules (or service rules) are the beginning of service processing. The service selection rules filter incoming requests and select the proper service for the request, because different types of network access requires different considerations when processing. Even though both APs and switches might send RADIUS requests to CPPM, CPPM will most likely need to process a RADIUS request associated with a WLAN differently from a RADIUS request associated with a wired connection. Similarly, it needs to process a RADIUS request for a corporate WLAN, which typically uses 802.1X, differently from a RADIUS request for a guest WLAN. This means that a different service needs to process each of these requests.

Service Rule Guidelines



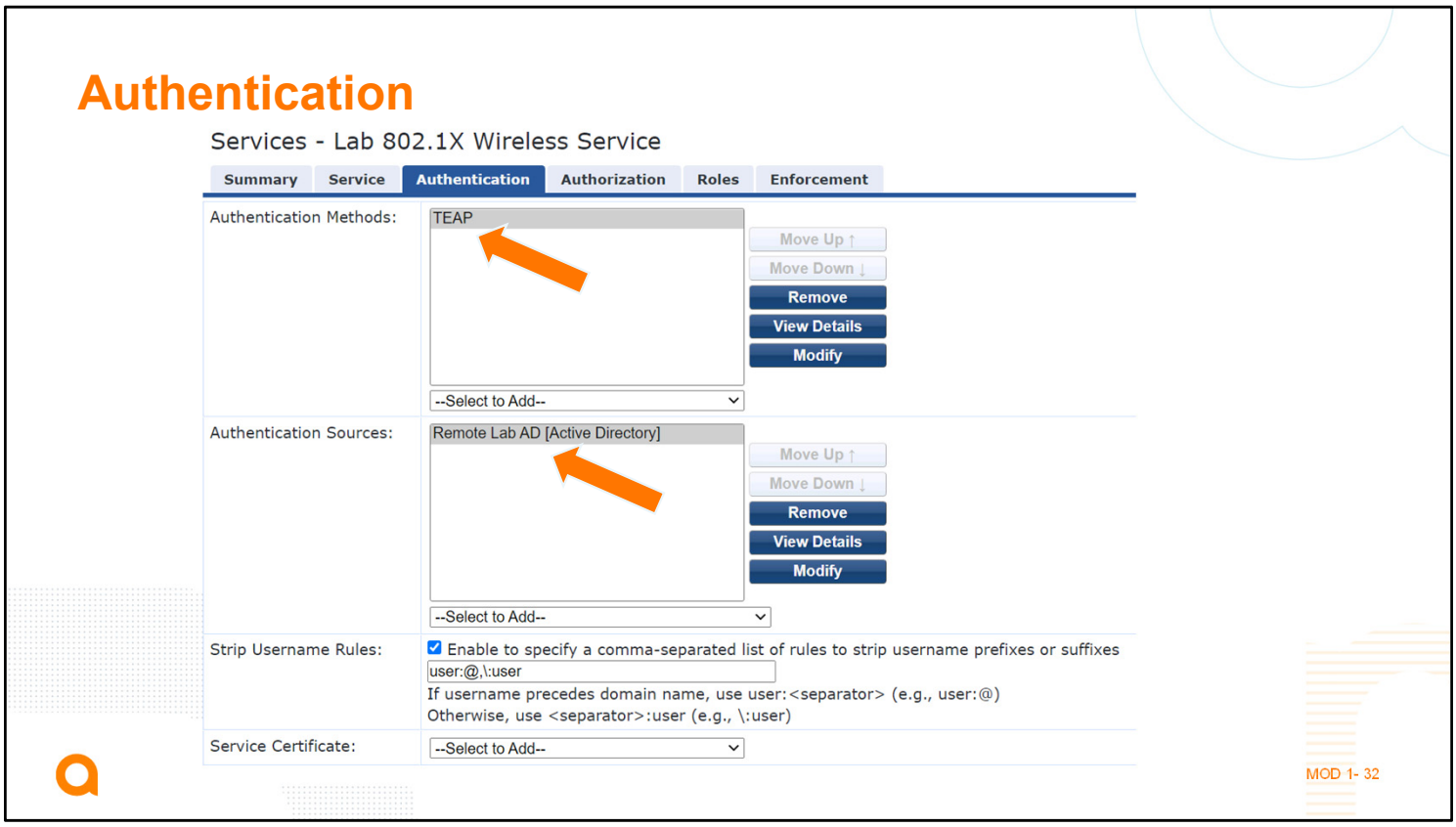
Even when you create a service from scratch, you can often select a service type, and CPPM will automatically create the correct service rules for that use case. However, it can still be useful for you to understand a bit about how a service rule is put together.

Each rule consists of four components. The type defines a “namespace,” or dictionary of attributes, while the name specifies the precise attribute. You can think of the attribute as a parameter. The value is a specific value for that parameter. The operator specifies the desired relationship between the value in the rule and the value in the actual request, in order for CPPM to say that a match has occurred. For example, does the value in the actual request need to equal the specified value exactly? Equal the value without regard to case? Start with a value? CPPM supports all these operators and many more.

Now look at how these components can combine together in some example service rules.

Many service rules use RADIUS attributes, which the network device includes as AVPs within the RADIUS Access-Request message. The namespace for these attributes can be “Radius:IETF” for standard attributes or “Radius:Aruba” for Aruba vendor specific attributes (VSAs). For example, in a wireless 802.1X policy, CPPM typically looks for the RADIUS Access-Request to specify the NAS-Port-Type attribute with a value of 19 for Wireless-802.11.

CPPM can also use AVPs within the access request to derive attributes in another namespace. For example, the RADIUS NAS-IP attribute indicates the network device’s IP address. CPPM stores information about all network devices, so it can use this IP address to determine the network device’s name or location. You can create rules that use these derived attributes as a more intuitive way to set up rules.

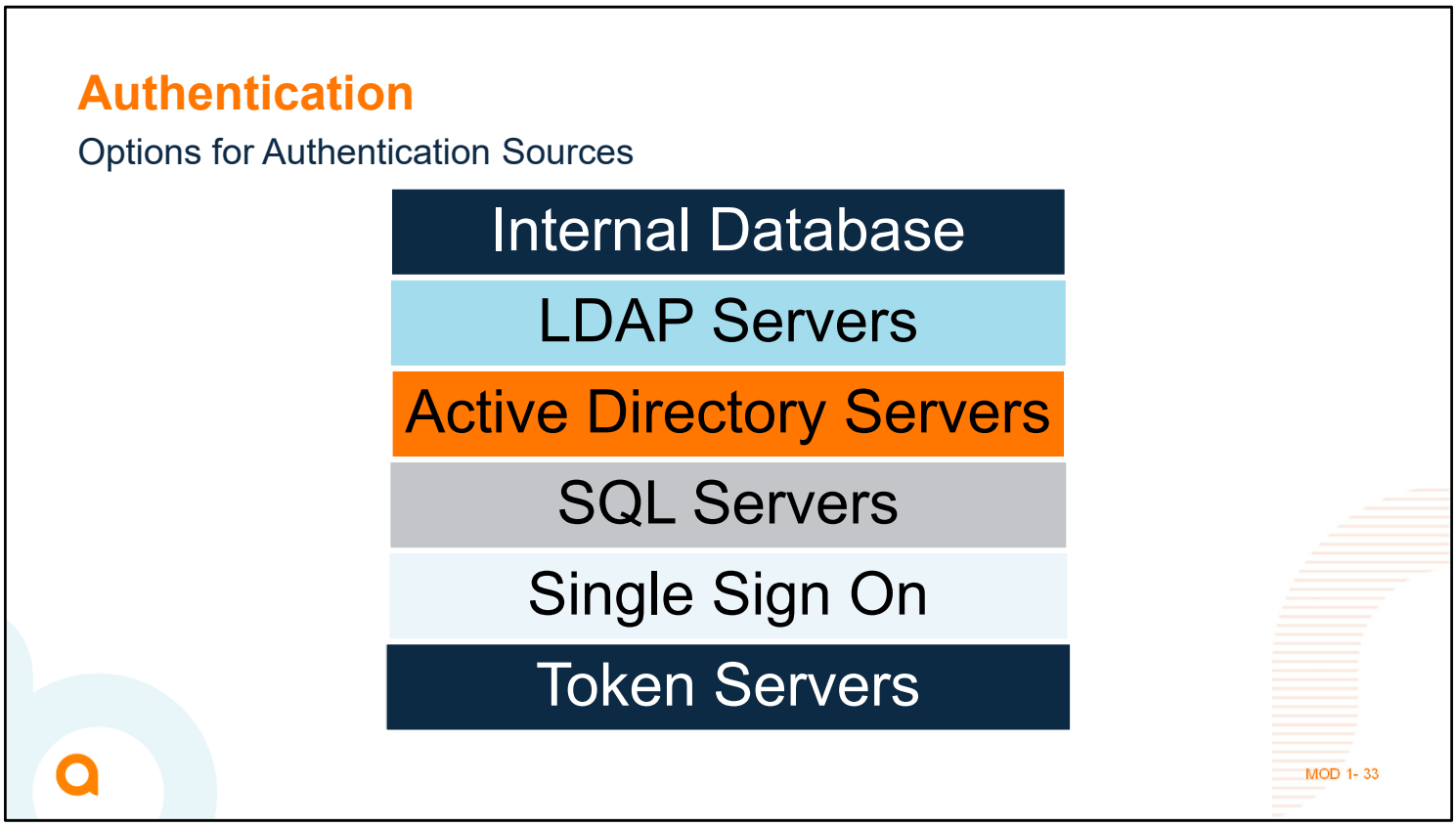


The next component of the service is authentication, and you specify the authentication settings in the Authentication tab. You need to select the valid authentication methods and authentication sources.

CPPM proposes each authentication method to the client in turn until the client accepts one of the methods. If the client does not support any of the methods, the authentication fails. Aruba recommends you clean up the Authentication Methods by reducing the list to only what is valid for the clients being authenticated by this service.

Assuming that the client does accept a method, CPPM uses the selected authentication method to collect the user's credentials. It then submits those credentials to the authentication source for verification.

You can select more than one authentication source. CPPM attempts to authenticate the client credentials against the sources in the list from top down.



CPPM uses authentication sources to validate the user's identity and credentials. The most basic authentication source is the internal database, which should be avoided except for use as a last resort. You may use it for a very small installation if necessary. LDAP servers, and specifically Active Directory servers, provide easy tools for managing accounts as well as rich context about the user. CPPM also supports SQL servers, single sign-on situations, and token servers, giving CPPM great versatility in authenticating users.

Question #3

Service Rules

What role do service rules play within a CPPM service?

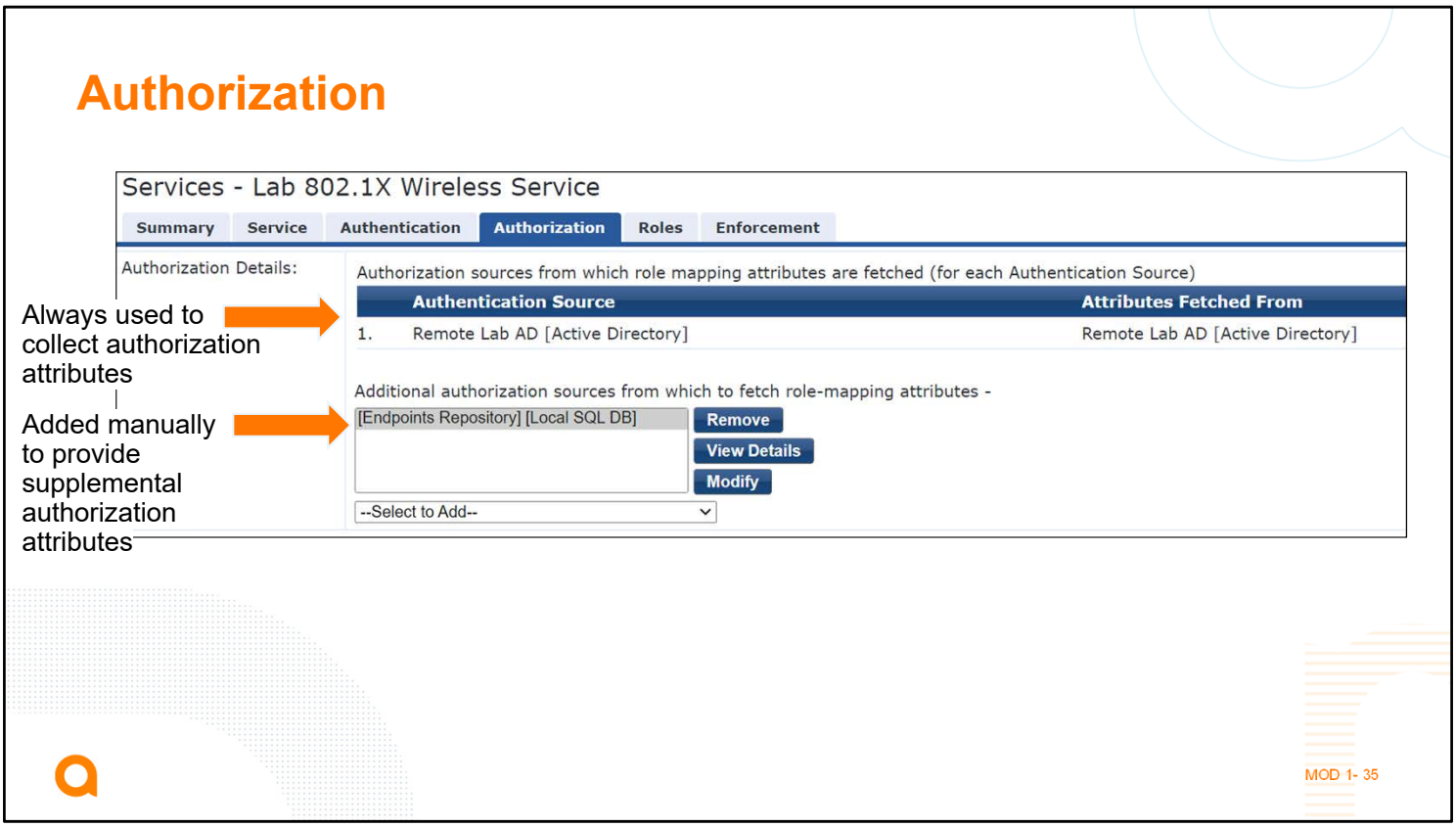
a. Determining whether a user is permitted access
b. Selecting the preferred authentication method
c. Matching the incoming request to the correct service
d. Determining whether the NAD is authorized

Knowledge Check

Take a moment to review what you have learned so far about CPPM services. What role do service rules play within a CPPM service? Select one.

Answer: C. Matching the incoming request to the correct service

Authorization



The Authorization tab for a service specifies the information sources from which CPPM will draw when it applies role mapping and policy enforcement policies.

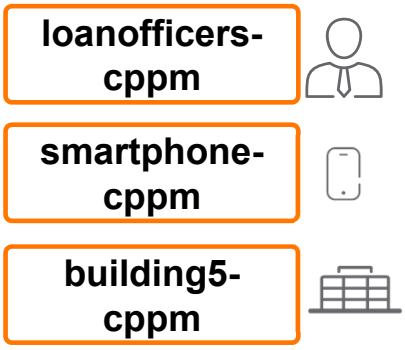
The first thing you'll notice in this tab is that the sources from the Authentication tab are added by default. This is because CPPM automatically authorizes against the authentication sources. In fact it collects authorization attributes from the authentication source even if you do not select the **Authorization** check box in the Service tab.

Sometimes the service requires input from sources other than the Authentication source. This includes things like endpoint context, timestamps, and even queries against a SQL database. To add these supplemental sources, you must first select the **Authorization** check box in the Service tab. The **Authorization** tab then appears. You can then go to that tab and add the desired sources.

What Is a CPPM Role?

- A descriptive tag
  - Any number permitted per client
- Context for enforcement policies

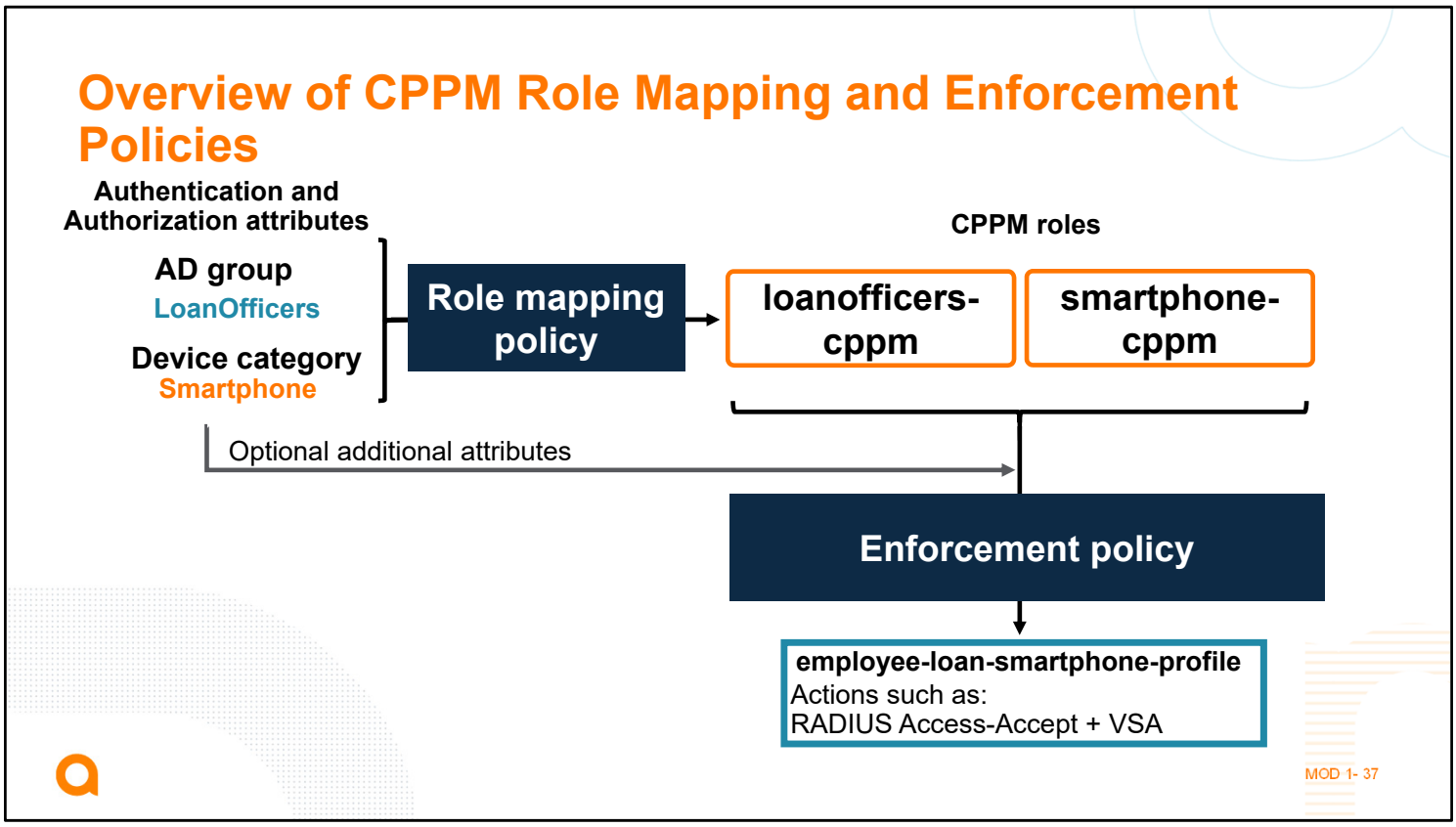
Example client's CPPM roles



MOD 1- 36

Having authenticated the user and collected information from authorization sources, the service is ready to start determining whether the client is permitted access to a network service and with what rights. This process generally starts with role mapping. Before you look at role mapping in detail, you should take a moment to learn what "role" means in CPPM and how CPPM roles are different from the "roles" that you might be familiar with on Aruba gateways, APs, and switches. As you know, a role on an AOS device is a group for assigning firewall policies and other settings to the client. Each client is assigned to only one role at a time.

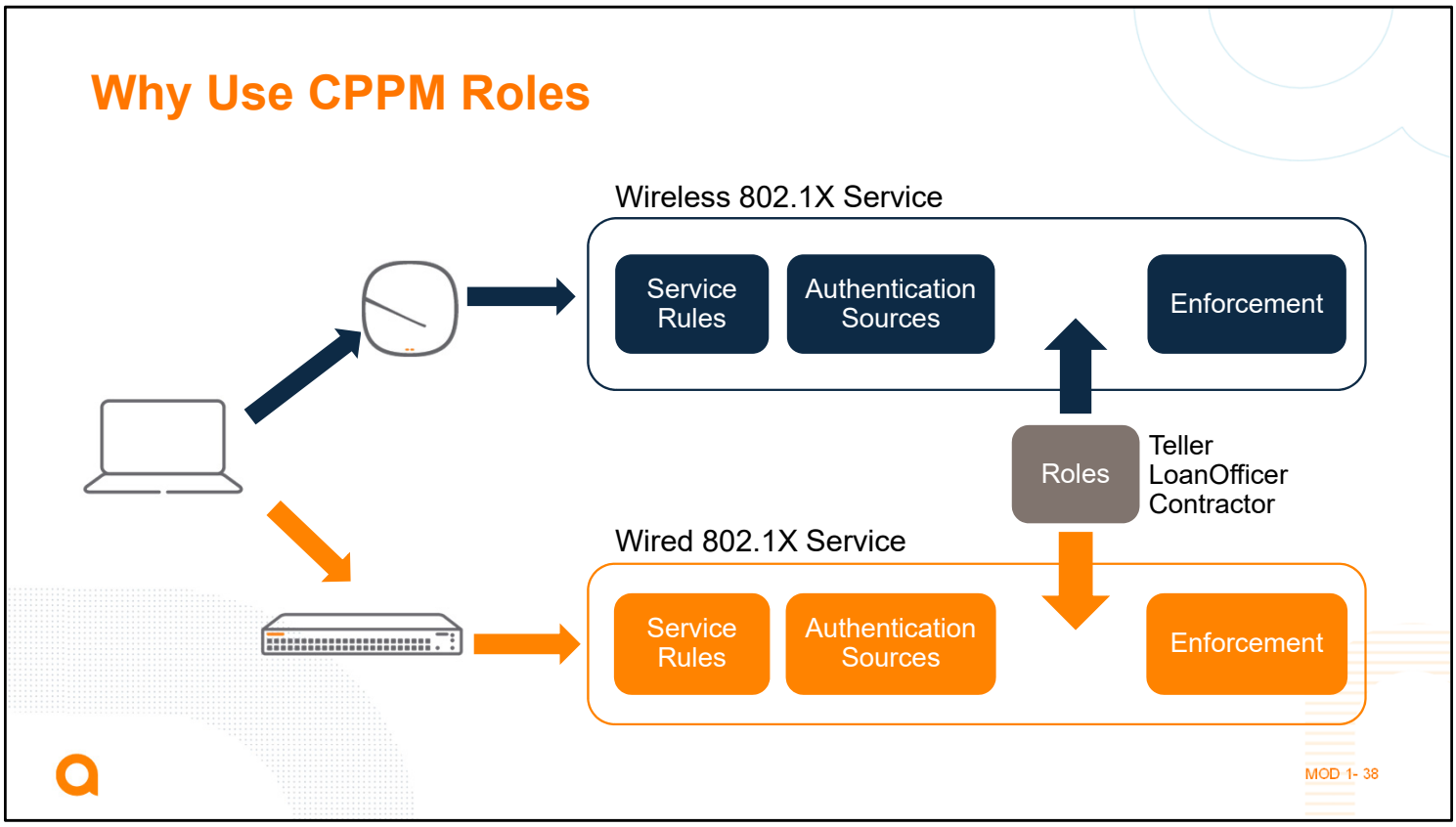
In CPPM, on the other hand, a "role" is simply a descriptive tag, which gives the service context about the client, including characteristics of both the user and the device. A CPPM role can describe the user's identity, such as indicating that the user belongs to the loan officer department. But the role can indicate other information as well. It can convey the device type. It can identify the client's location. You can create any CPPM roles that you want to convey the information that is important for your organization's policies. And CPPM can assign multiple roles to the same client in order to build up a complete picture of the user and device.



CPPM primarily assigns roles to clients based on rules within role mapping policies. Those rules draw on authorization attributes collected during the authorization stage of the service processing. Two examples are shown here, but many other examples exist. After the role mapping policy finishes processing, the client has one or more roles assigned to it.

You can then use the roles as conditions in rules within an enforcement policy. You can also optionally include other authorization attributes in the enforcement policy rules. Each rule applies one or more enforcement profiles to clients that match the rule.

The enforcement profile defines actions to apply to the client. For example, the profile might tell CPPM to send a RADIUS Access-Accept message to the authenticator, as well as to include VSAs to customize the client's access.



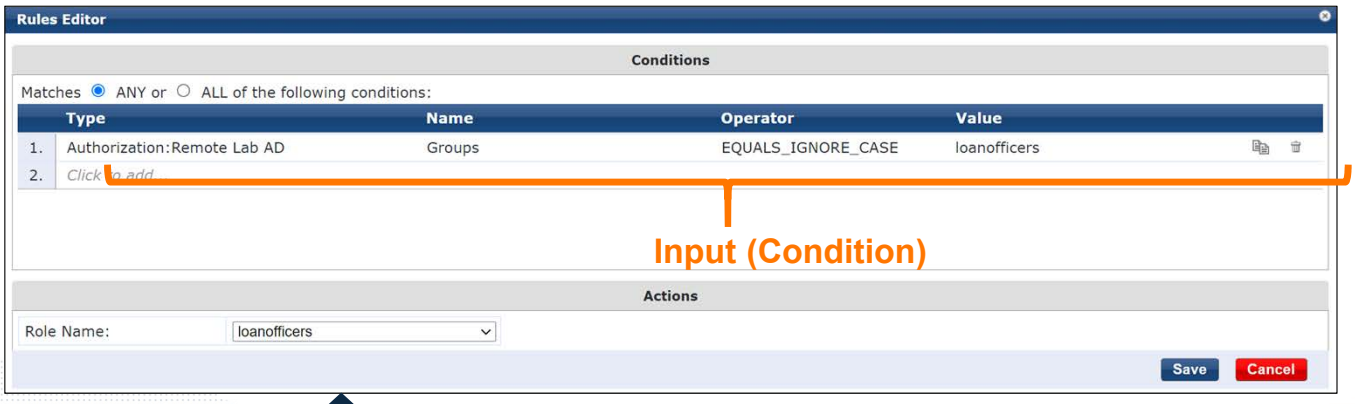
The biggest advantage to using roles in CPPM is in bringing consistency across multiple services. Once the organization is able to define how to describe a client, you can implement the rules in a universal role mapping, which you can then use in all services.

In this example, the same client might attempt to connect to either the wired or wireless network. The client authentication needs to be processed by a different service depending on the connection type because a different enforcement profile is required for enforcing access on the wireless versus the wired network infrastructure device. However, by using the same role mappings, the client will always be categorized in the same way. The difference comes in how CPPM communicates this categorization to the network infrastructure device. This approach makes enforcement more consistent.

In other words, the role defines the client while the enforcement policy defines how to treat the client.

CPPM can assign multiple roles to a client, indicating that the client meets multiple conditions.

Overview of Role Mapping Rules



CPPM primarily determines which roles to assign to a client based on rules within the service's role mapping policy.

Before you look at role mapping and enforcement policies in more detail, it will be useful to examine the general format for these policies' rules.

Every rule has a type. The type defines the namespace dictionary from which information about the user or client is retrieved. CPPM supports many namespaces. In this course, though, you will focus on just a few commonly used namespaces. For both role mapping and policy enforcement rules, you can use the authorization namespace, which is further defined by a particular authorization source. For example, you are using AD as the authentication source and authorization source. You can select the dictionary of attributes collected from AD by specifying "Authorization:<*AD instance name*>" for the type.

Next the rule defines a name, which is an attribute in the namespace dictionary that you selected for the type. For AD instances, these are generally attributes stored within the account. You define which attributes to collect when you define the AD authentication source. The "Groups" attribute is often used to define a client by the user's AD group membership.

Next the rule defines an operator and a value. The operator links the attribute to the value. For example, you could create this rule: "Authorization:AD_instance Groups EQUALS_IGNORE_CASE Teller." CPPM then checks the "Group" attributes that it collected for each user, and it applies this rule if the attribute equals "Teller" or "teller." In other words, it applies the rule if the user is in the Teller group.

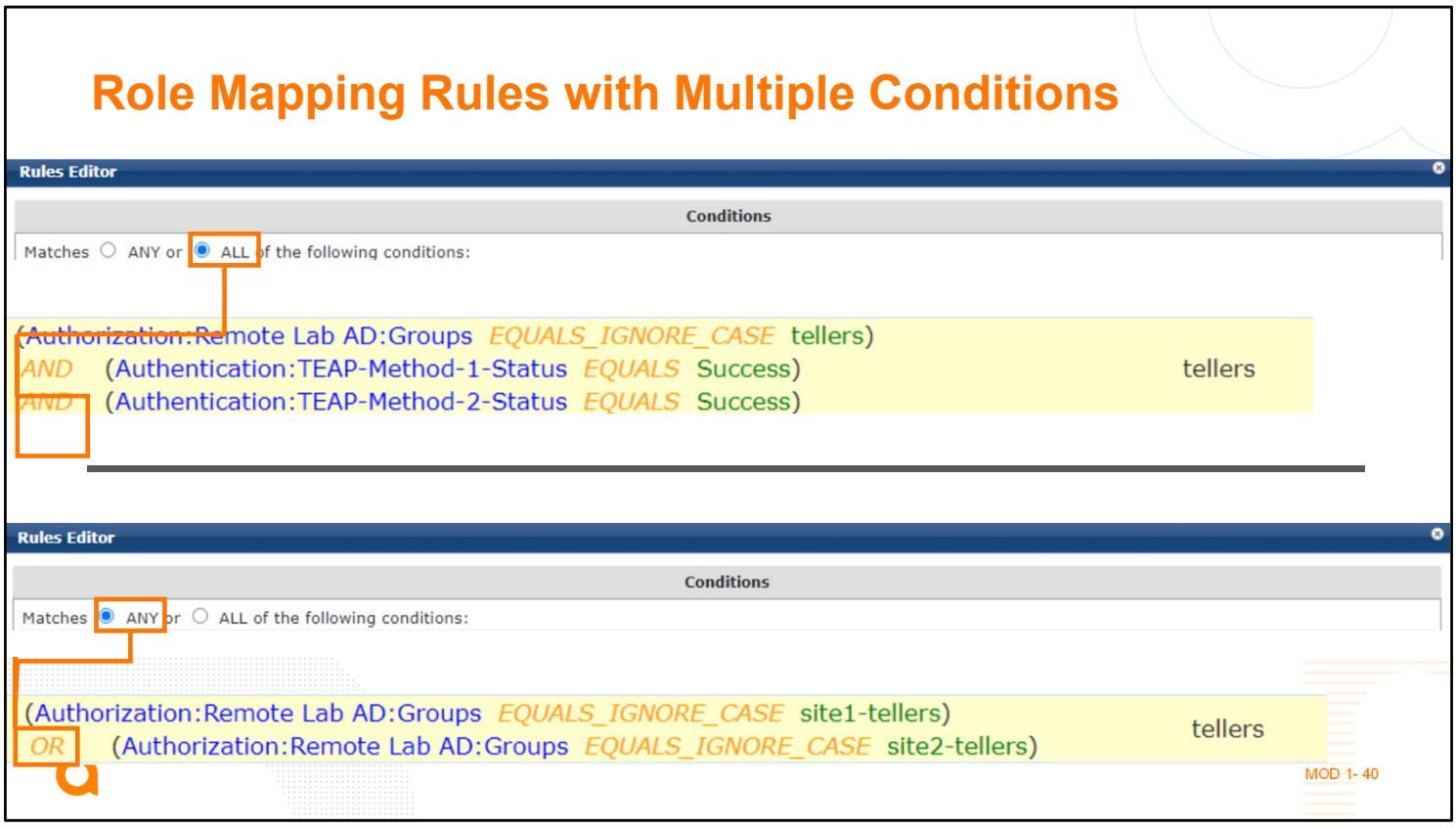
CPPM supports many other operators to enable you to create flexible rules. For example, you could use "STARTS_WITH" to match multiple attribute values, all of which start with a specific string.

Those four components create the condition.

Finally, the rule specifies an output—a decision for CPPM to support. For a role mapping rule, the output is a CPPM role. For an enforcement policy rule, the output is an enforcement profile.

—

For a complete list of namespaces supported in CPPM v6.9, refer here: https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/CPPM_UserGuide/Rules/Namespaces_RADIUS.htm?Highlight=namespace



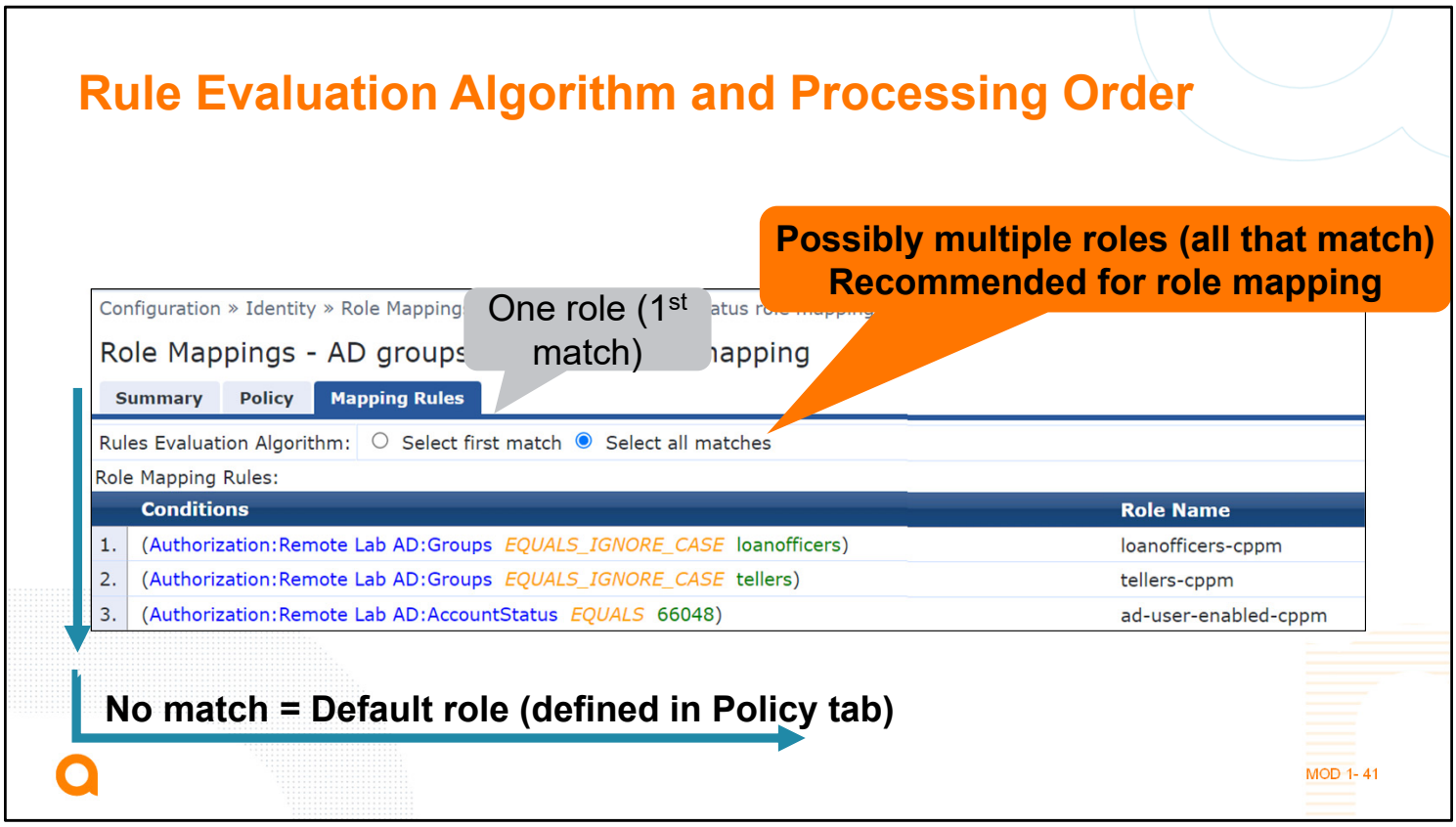
You can also create more flexible rules which include multiple sets of conditions.

When you create the rule, you can choose that all conditions must be matched. This option creates an AND between the conditions.

Or you can choose that the client can match any of the conditions. In this case, conditions are separated by OR. In other words, the client receives the role if it matches any one (or more) or the conditions.

—

The second rule shows a condition in which a client receives a role if it belongs to either one of two AD groups. In the example shown here, you could achieve the same effect with one condition that uses the operator CONTAINS. However, this rule serves to provide an example of how the OR operator works.

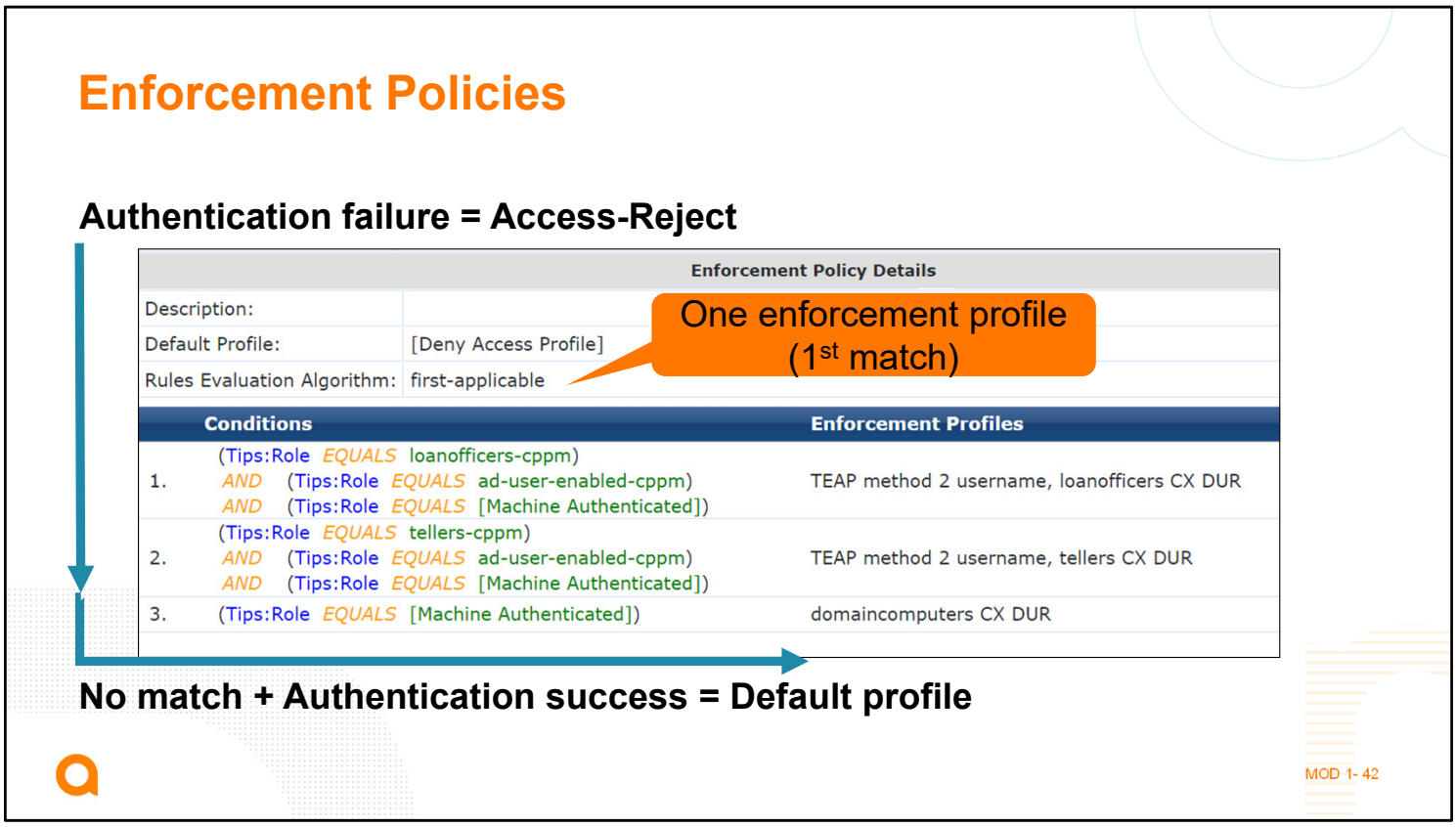


CPPM processes policies in order from the top rule to the bottom.

For role mapping policies, you can choose whether CPPM should “Select First Match” or “Select All Matches.” Use “Select First Match” when you want each user/client to receive a single role. In this case, CPPM assigns the user/client only the role from the first rule that matches. So you need to pay attention to the order in which you define roles.

Use “Select All Matches” if you want CPPM to assign multiple roles to the user/client based on various information about the client. For example, you could assign a user on a managed domain client to two roles: one role based on AD group membership and one general role for all users on managed clients. Aruba generally recommends using the “Select All Matches” option for role mapping policies. Then you can assign as many roles as might be required to each client to fully characterize it. The roles will not have any effect until you use them in enforcement policies

If CPPM does not find a matching rule at all, it applies the default role, which you define in the Policy tab.

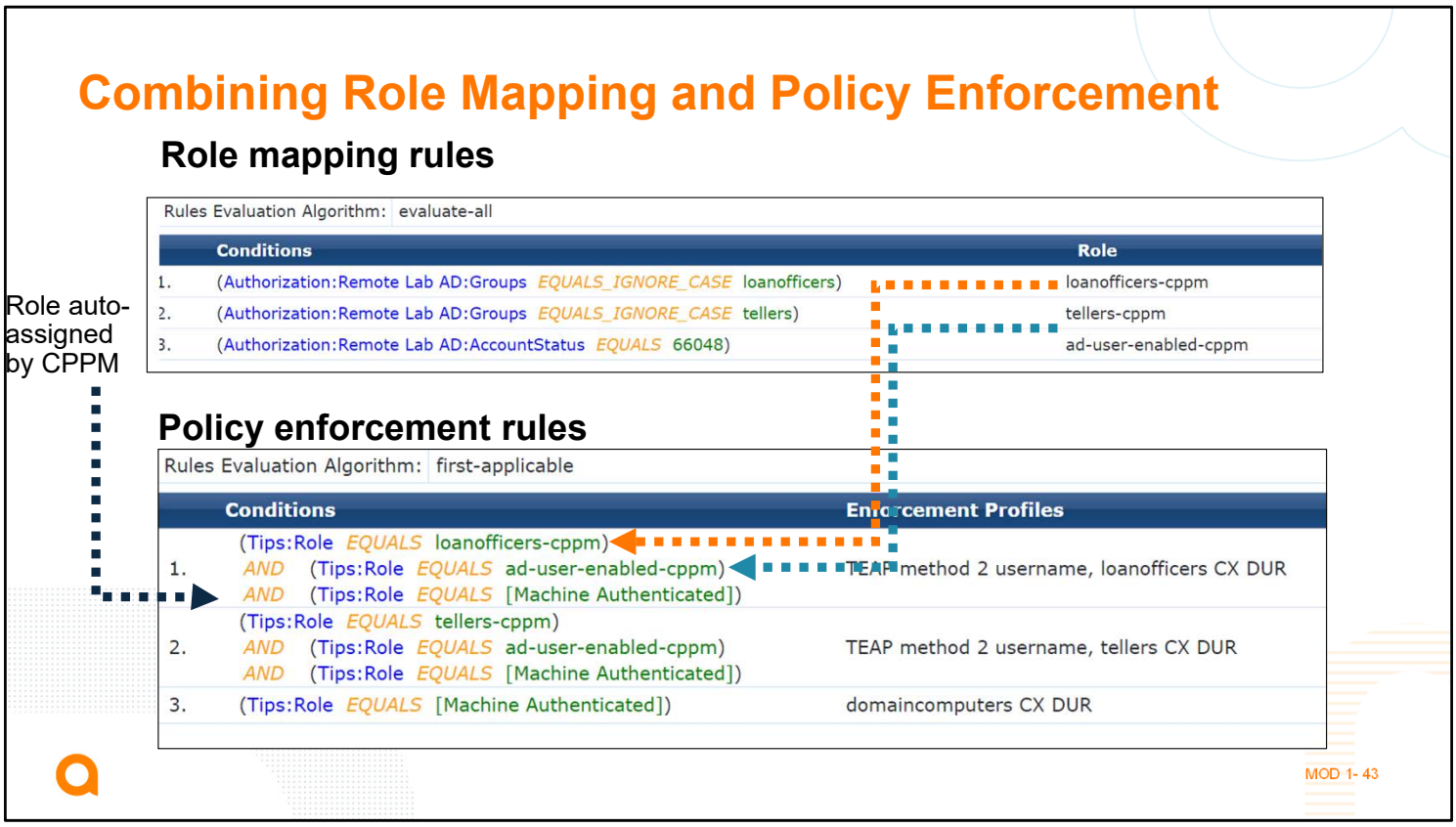


The general format for enforcement policy rules is very similar to role mapping rules. However, additional types and names (namespaces and attributes) are available for enforcement policy rules. For example, you can create a rule based on a CPPM role by specifying “Tips” for the type and “Role” for the name.

The output, or action, for an enforcement policy rule is an enforcement profile or multiple enforcement profiles.

For enforcement policies, Aruba recommends setting the Rules Evaluation Algorithm to First Match. CPPM then evaluates the rules from top to bottom and applies only the first rule that matches the client.

If no rules match, but the client did pass authentication, CPPM applies the default profile. Often, but not always, you should set up the default profile to deny access. If the client fails authentication, CPPM always sends an Access-Reject regardless of the default profile setting.



Here you see an example of how you can combine role mapping and policy enforcement policies.

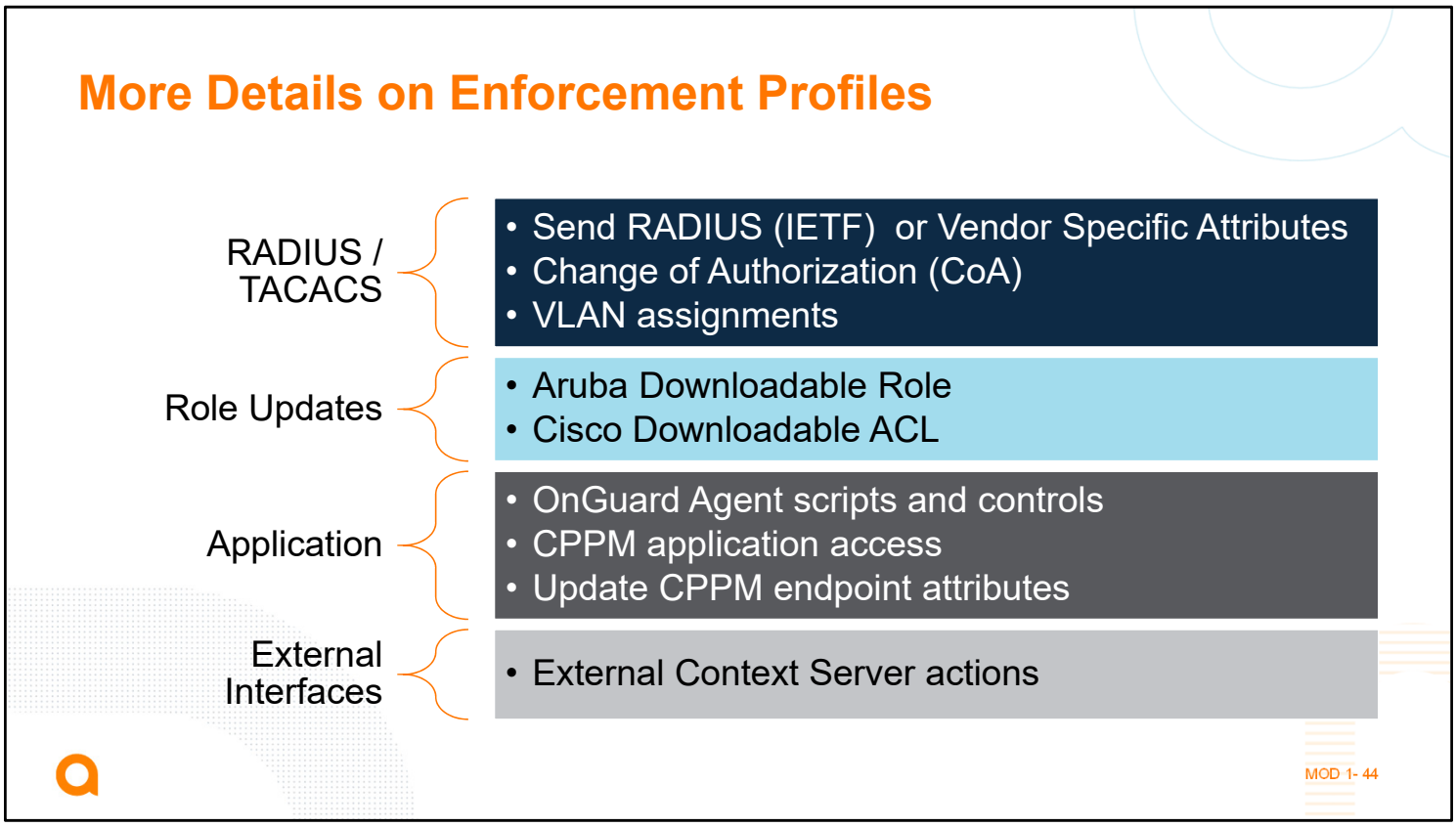
The role mapping policy takes an "evaluate-all" approach and assigns clients to every role that applies. In this example, users receive either the "loanofficers-cppm" or "tellers-cppm" role based on AD group. They might also receive the "ad-user-enabled-cppm" role based on their account status.

CPPM can also assign clients to two roles without the use of a role mapping policy. These rules are [User Authenticated] for clients that have authenticated with a user account and [Machine Authenticated] for clients that have authenticated with a computer account. A client might have both roles if a user has authenticated on a client that also authenticated as a machine.

The enforcement policy has rules that combine these roles together to produce an output. For example, you might apply a particular enforcement profile to clients that have achieved multiple roles.

Rule 1 in the figure shows an example. It has several conditions joined by the "AND" operator. For each condition, the namespace is "Tips," which indicates CPPM-derived information. The attribute is "Role." The operator is "EQUALS," and the value is the role in question.

This example rule outputs several enforcement profiles.



As you just saw, as the service finishes processing, CPPM applies an enforcement profile to the user/client.

The enforcement profiles define how CPPM takes action. CPPM has many enforcement actions, making it very powerful and flexible.

The previous example showed a common enforcement profile type: RADIUS. With this type, CPPM sends a RADIUS message that tells the authenticator to accept or reject access. An Access-Accept message can further customize the access with settings such as VLAN or role assignments. TACACS profiles similarly tell CPPM to send a TACACS message to permit or deny user access and specify the authorization level.

Enforcement may also include situations in which CPPM formulates a User Role or ACL and then sends it to the network access device.

You can also use SNMP or CLI commands to control various aspects of the network devices. For example, if a wired IoT client fails MAC authentication, CPPM could execute the commands for a port shutdown to remove that client from the network.

Similarly CPPM can control clients by imposing session restrictions, such as a session-timeout or re-authentication interval. With some Network Access Devices (NADs), CPPM can execute a captive portal or external web redirect to the client. This is helpful with network access devices that do not natively support external web authentication or redirection when the client has already authenticated.

Often you will need to build services to control which clients have access to CPPM applications such as Onboard or OnGuard. CPPM can also interact with the OnGuard agent to execute controls on the clients. CPPM can update endpoint information, giving context to previous endpoint activity. For example, what if a company does not want client devices on the corporate network to access the guest network? The company can use a CPPM Entity Update Enforcement action to tag a device as

a corporate client. In this way, when a corporate client attempts to access the guest network, the guest access service reads the attribute and denies access to the guest network.

CPPM can also interface with external services and servers to exchange context information about a client accessing the network.

Question #4

What is a reason to use role mapping policies?

a. Because role mapping policies simplify configuration by eliminating the need for enforcement profiles and policies
b. Because you want to characterize clients with a global policy that you can use in multiple services
c. Because you want to use more complex conditions which are not supported in enforcement policies
d. Because you want to define role-based firewall policies directly within CPPM

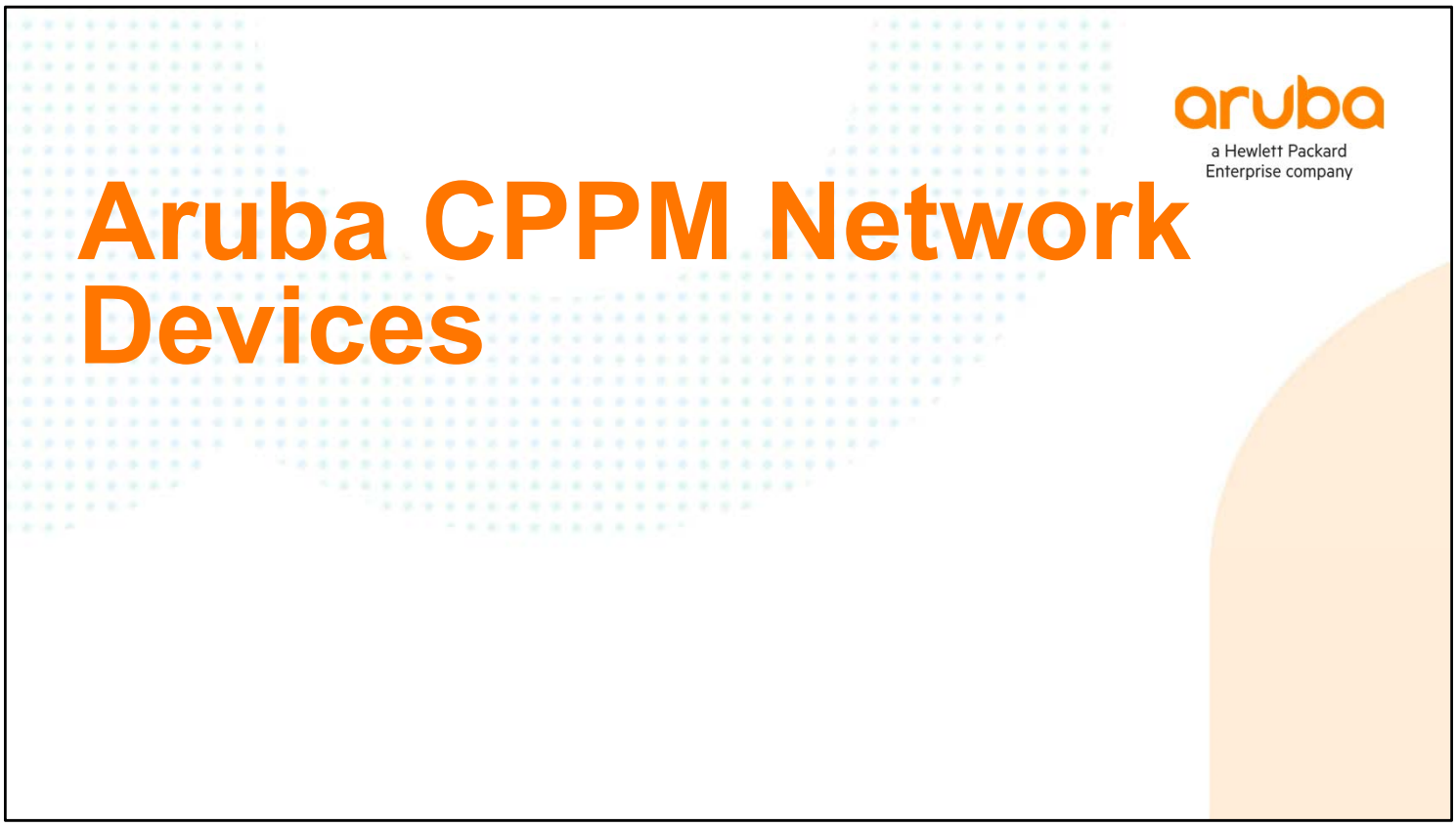
Knowledge Check

Take a moment to review. What is a reason to use role mapping policies?

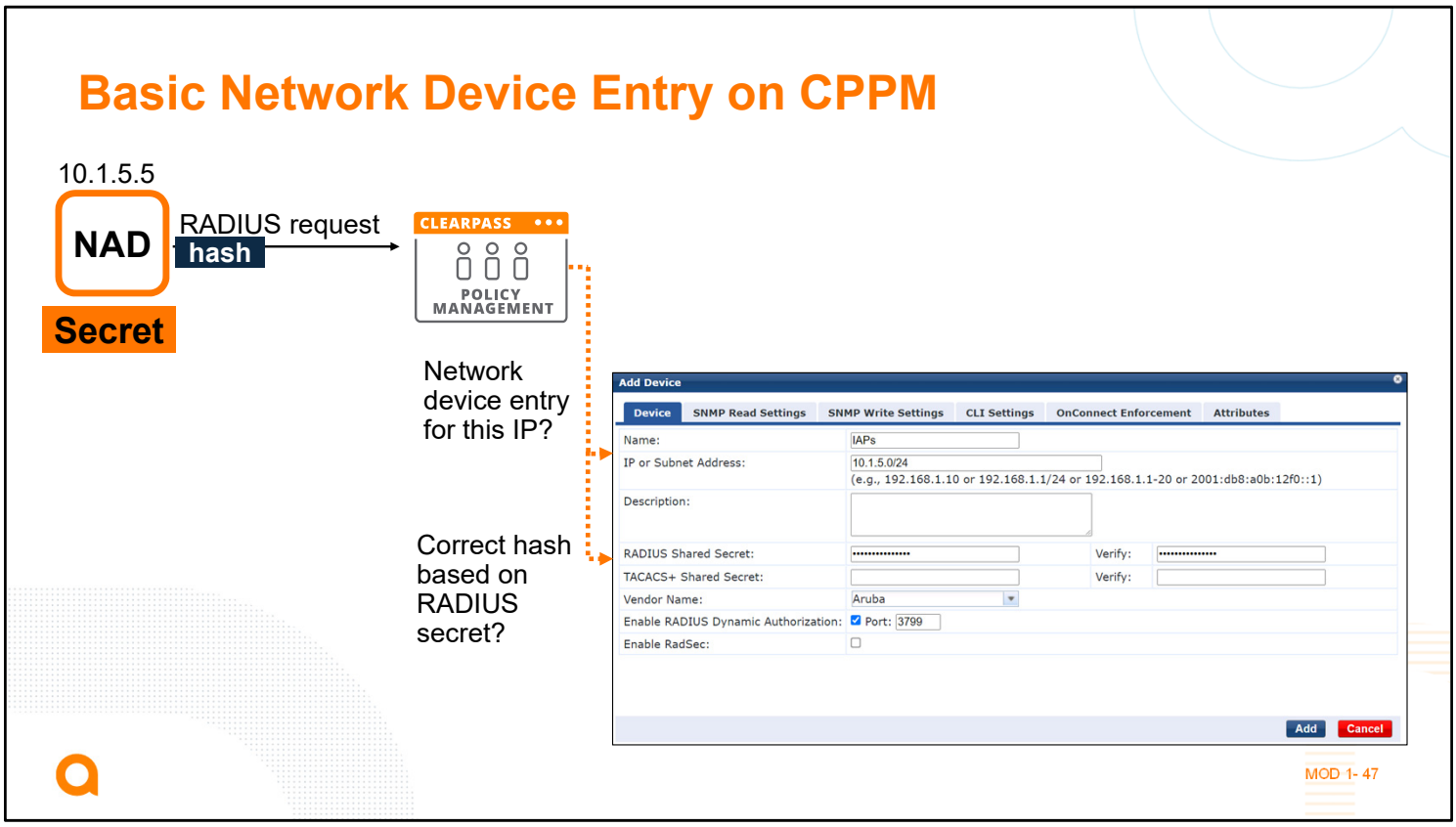
Select one.

The answer is:

Because you want to characterize clients with a global policy that you can use in multiple services



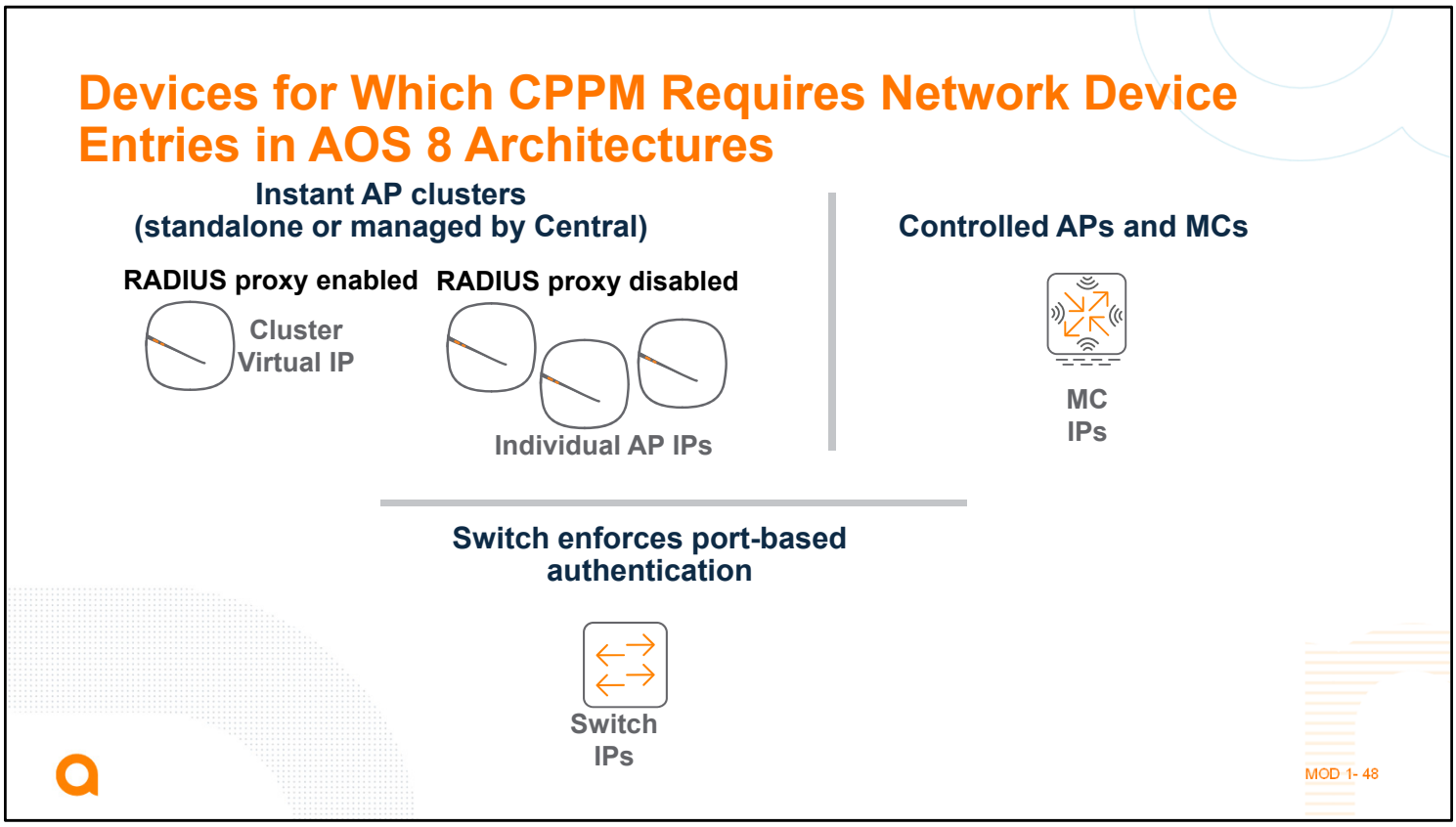
Topic 4: Aruba ClearPass Policy Manager (CPPM) Network Devices



For CPPM to accept RADIUS requests from a NAD and process those requests with a service, you must create a network device entry for that NAD on CPPM.

Here you see a basic network device entry. The entry specifies a single IP address or a complete IP subnet. When CPPM receives a RADIUS request, it checks the source IP address for the request and matches it to a network device entry with that address. In this example, the request arrives from 10.1.5.5, so it matches a network device entry with Subnet Address 10.1.5.0/24. If no entry exists for the IP address, CPPM drops the request (and logs the event in the Event Viewer). Therefore, you must make sure that you understand the IP addresses that your network infrastructure devices will use to reach CPPM and create entries for them.

The network device entry also includes a RADIUS shared secret. You must match the secret configured here in the RADIUS server configuration on the NAD.

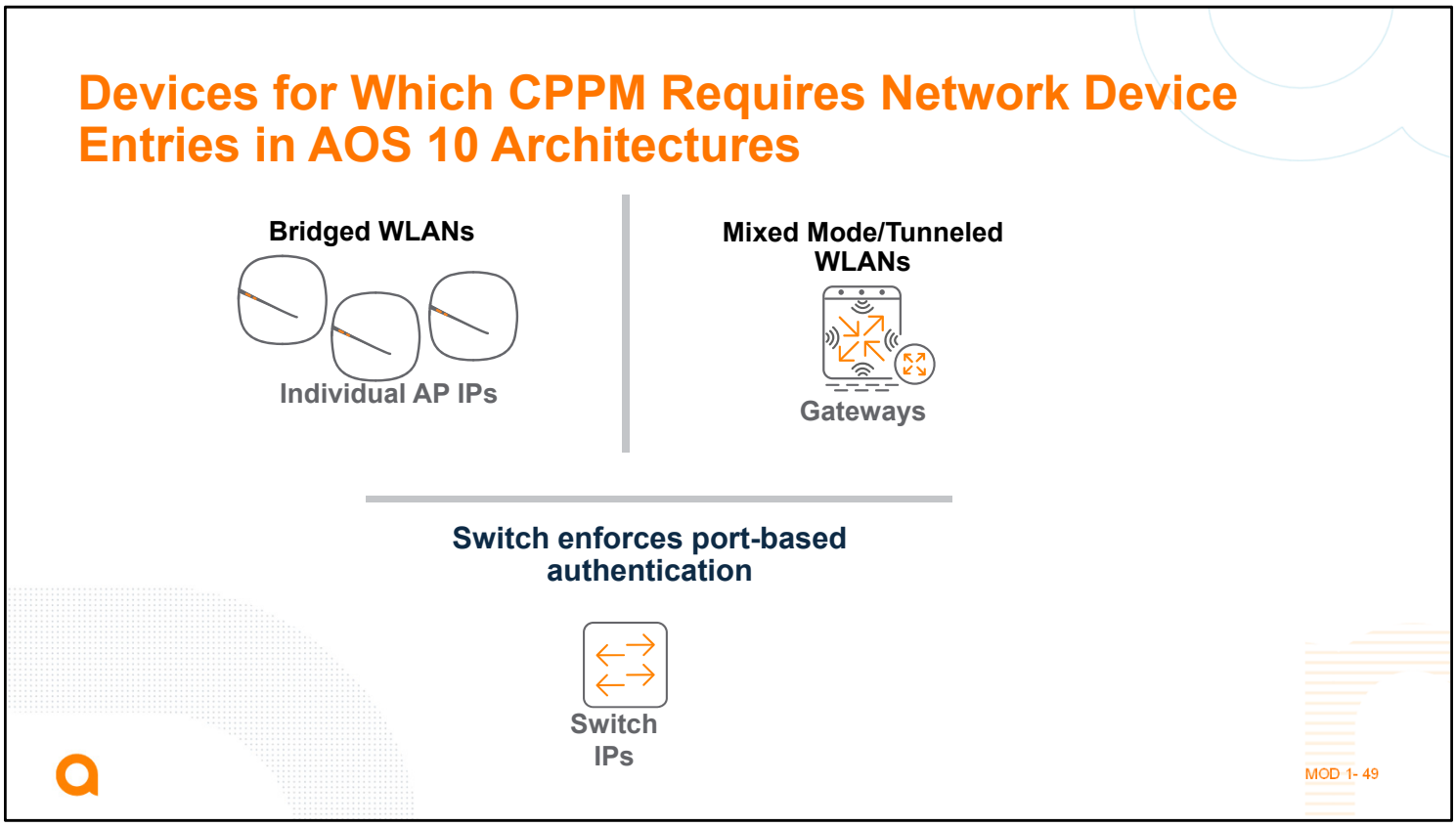


To create the correct network device entries, you must understand which network infrastructure devices take the NAD role in your architecture.

In an AOS 8 architecture, mobility controllers (MCs) act as NADs and authenticate wireless clients to CPPM. Therefore, you must create network device entries for the MCs on CPPM.

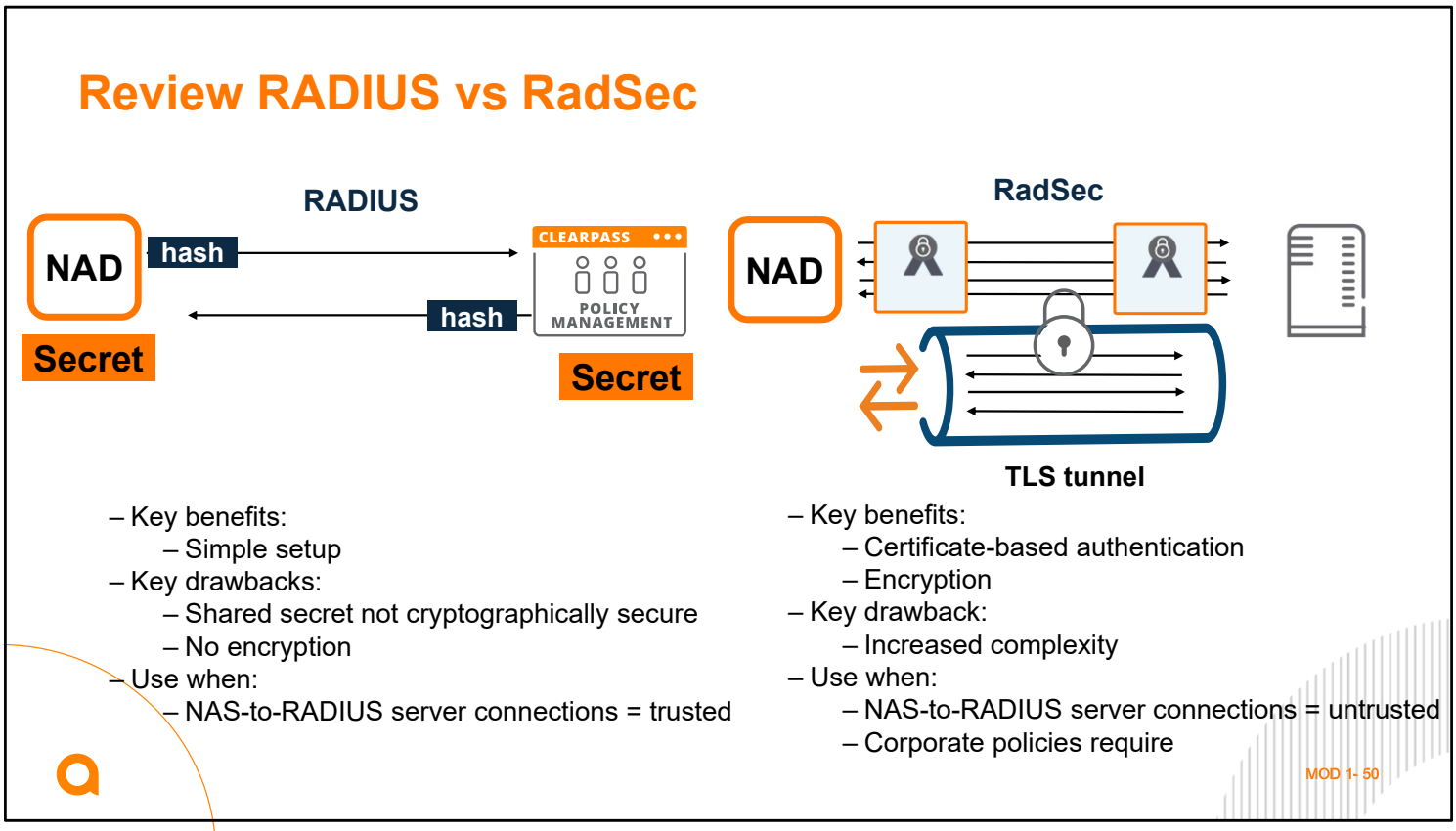
In an Instant AP cluster, which might be standalone or managed by Central, the APs within the cluster might act as NADs. If RADIUS proxy is enabled on the cluster, though, the APs send their RADIUS requests through the virtual conductor. CPPM only needs a network device entry for the cluster's virtual IP address. However, if RADIUS proxy is disabled, it needs an entry that applies to all of the APs.

Aruba switches can also act as NADs in any of these architectures. When you configure port-based authentication on the switch, it is the NAD, and CPPM requires a network device entry for it.



APs act as NADs for wireless clients in AOS 10. When the WLAN operates in bridged mode, the APs use their IP addresses for the NAS IP address. When the WLAN operates in mixed mode or tunneled mode, the gateway acts as the RADIUS proxy. You then need to add a network device entry for the gateway in CPPM.

In AOS 10 architectures, as well, Aruba switches might implement port-based authentication, in which case CPPM must have network device entries for them.



As you learned, network devices and CPPM communicate with RADIUS during the process of authenticating clients for network access. You can implement RADIUS alone or add a layer of security with RadSec.

RADIUS

RADIUS uses a shared secret to authenticate the RADIUS client (NAD) and RADIUS server to each other. You must configure a matching shared secret on both devices. The NAD and server include a hash of the message and shared secret within all RADIUS messages. If the hash does not check out, indicating that the secret is incorrect or that the message was tampered with, the receiving device drops the message. However, the shared secret does not provide rigorous security. You can make it more secure by setting a very long, random key. However, RADIUS itself is not considered a secure protocol. It also transmits data in plaintext.

You should only run RADIUS over trusted network connections. For example, if network devices and CPPM are deployed at the same site, you can generally use RADIUS between them. You can also use RADIUS between network devices and CPPM servers at another site if the site-to-site connection is secured with a protocol like IPsec.

RadSec

RadSec establishes a TLS tunnel between the RADIUS client (NAD) and RADIUS server. During the TLS tunnel establishment, the NAD and RADIUS server authenticate each other with certificates. After the TLS tunnel comes up, the NAD and RADIUS server exchange all RADIUS messages over the tunnel, including authentication and accounting. The tunnel provides encryption and data integrity for the messages. Because the tunnel uses TCP, rather than RADIUS's typical UDP, the NAD can also detect when it loses contact with the RADIUS server more quickly.

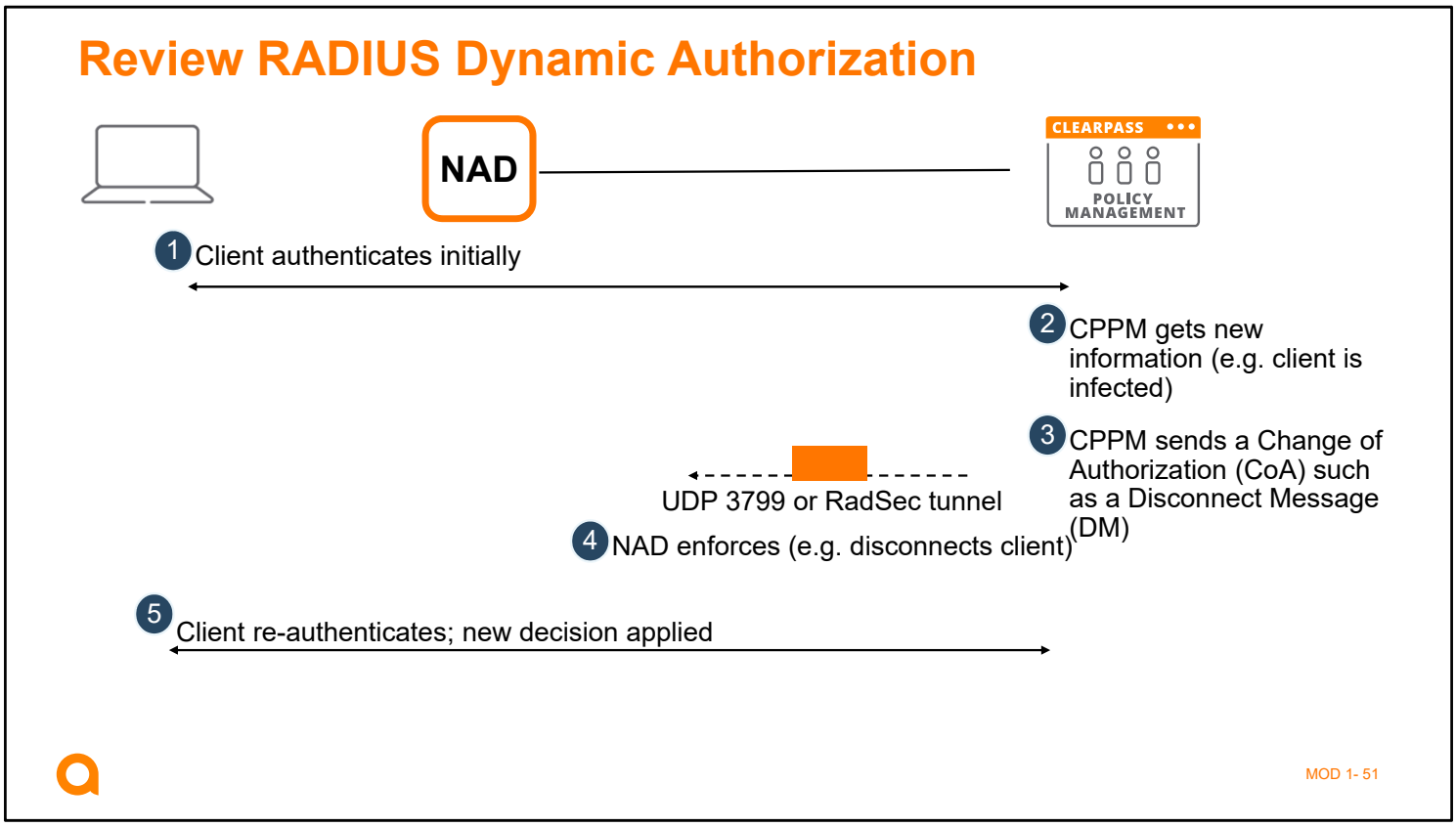
When you enable RadSec on the NAD or on CPPM, the RADIUS secret is automatically set to

"radsec." Instead you set up certificates to provide the authentication. You will learn more about this process later in this course.

RadSec provides greater security than RADIUS, but the certificate requirements can make it harder to deploy and maintain. Issues can occur such as a NAD's certificate expiring. Aruba recommends RadSec when network devices and CPPMs must communicate over untrusted network connections. Some companies also require RadSec as part of their security policies.

—

Network devices can also use TACACS+ to authenticate managers to CPPM. You will learn more about TACACS+ later.



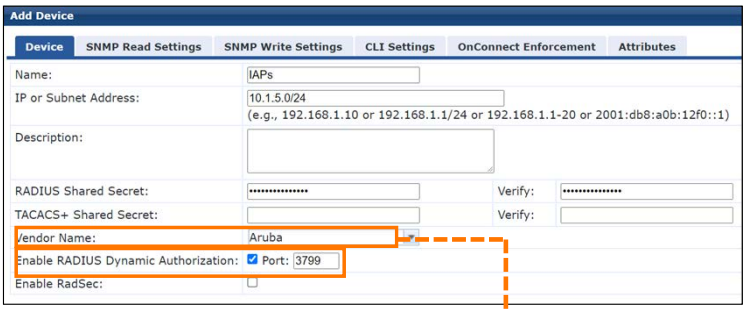
A RADIUS server like CPPM is capable of making decisions about a user's or device's authorization beyond the initial authentication. For example, ClearPass Onguard can detect a client's security posture and tell CPPM to disconnect a client that does not have the proper firewall and antivirus settings. Or CPPM might find out after the initial authentication that the client is an IoT device, which has particular security policies associated with it. Many other examples of such events exist.

So that CPPM can enforce the new policies, it must force the client to disconnect and re-authenticate. It sends a Change of Authorization (CoA) message to the NAD such as an AP, switch, gateway, or MC. By default, CPPM sends the message on standard port UDP 3799. But you can change that port, as long as you match the setting on CPPM and the NAD. If CPPM and the NAD are using RadSec, CPPM sends the CoA messages in the RadSec tunnel.

When the NAD receives a CoA from an authorized dynamic authorization server, it enforces the message and disconnects the client. The client will typically try to re-authenticate, and CPPM can then apply its policies to make new decisions about the client's access.

Enabling Dynamic Authorization in a CPPM Network Device Entry

Network Device on CPPM



Determines which CoA enforcement profiles are valid

Corresponding config on the NAD

Enable in RADIUS server settings

1. Add a separate RFC 3576 server with CPPM's IP
2. Add that server to the AAA profile

1. Enable dynamic authorization
2. Define CPPM as a dynamic authorization client

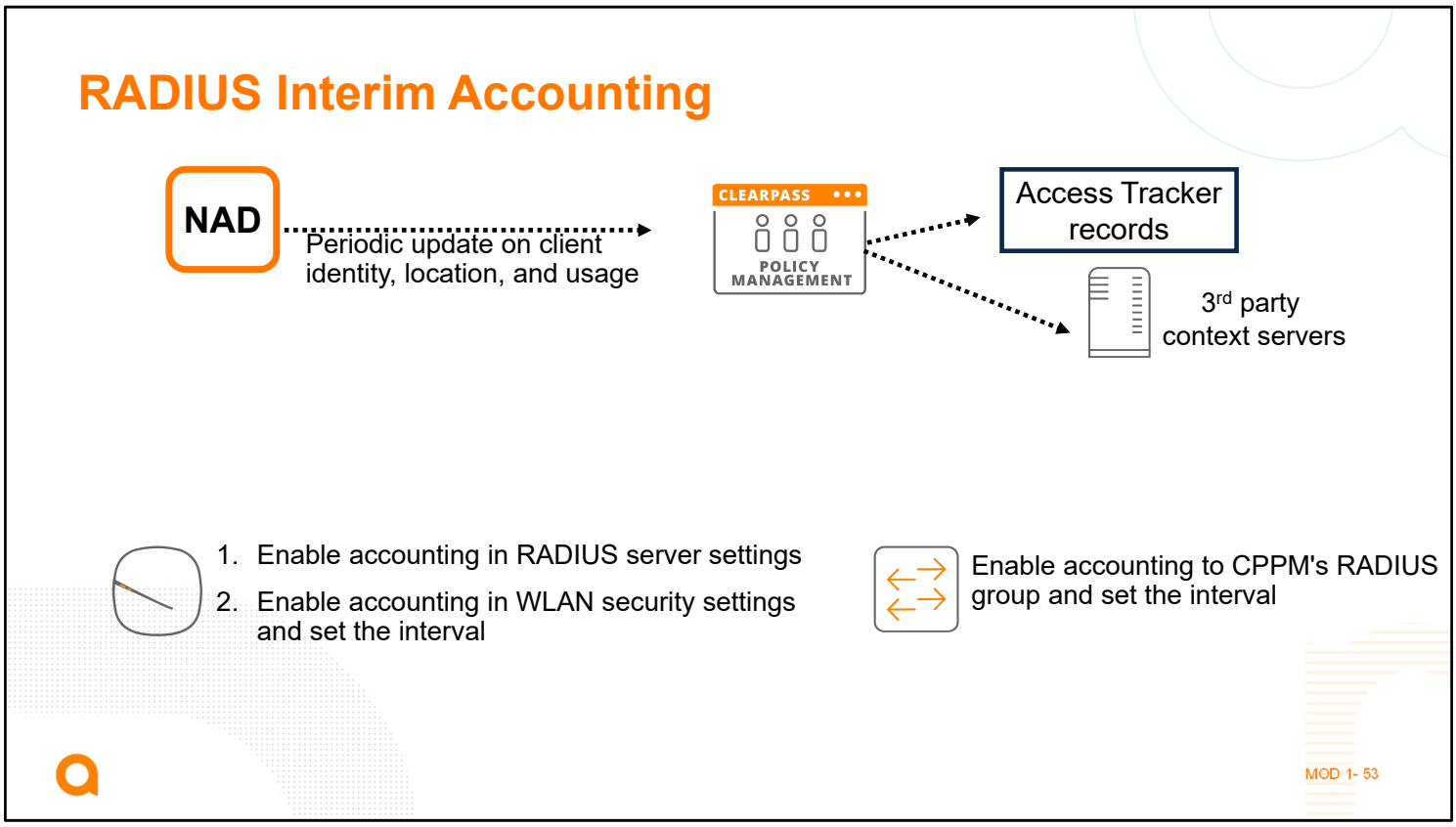
MOD 1- 52

To enable the CoAs, you must make sure that CPPM's network device entry for the device in question has **Enable RADIUS Dynamic Authorization** enabled. Also note the Vendor Name. CPPM uses CoA enforcement profiles to trigger the CoAs. It has different enforcement profiles for devices from different vendors. The vendor name within the network device entry helps CPPM determine whether a profile is valid for a particular network device, so make sure to set the name correctly. The vendor name also enables the correct VSAs for the network device. Use **Aruba** for Aruba APs, MCs, gateways, and AOS-CX switches.

Similarly, you must make sure that the network device is configured to accept CoA messages. On IAPs you enable **Dynamic Authorization** in the RADIUS server configuration.

The setup on gateways (or MCs) has a few more steps. Instead of enabling dynamic authorization on the RADIUS server, you set up a separate Dynamic Authorization server with CPPM's IP address. You set a key for the Dynamic Authorization server that matches the RADIUS key in CPPM's Network Device entry for the gateway or MC. (If you are using RadSec, the key is "radsec.") You then activate the Dynamic Authorization server in the AAA profiles that the device is using to authenticate clients to CPPM.

On AOS-CX switches, you also define the CoA settings separately from the RADIUS server. You must enable dynamic authorization with this command: **radius dyn-authorization enable**. Specify CPPM's IP address as a dynamic authorization client on the switch with this command: **radius dyn-authorization client <*CPPM IP or FQDN*>.**



As an AAA protocol, RADIUS not only provides authentication and authorization, but also accounting. RADIUS accounting logs a broad range of information such as a client's username, NAD port, and bandwidth consumption in packets and bytes. A NAS can implement RADIUS accounting in these modes:

Stop—When the client's session terminates, the NAD sends a message that summarizes the session

Start/stop—The NAD sends an accounting message at the beginning of the session and then a session summary at the end.

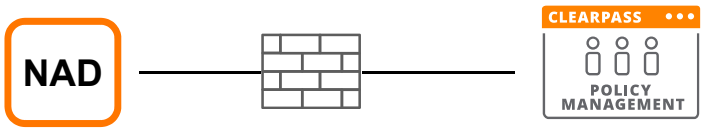
Stop or start/stop + interim accounting—The NAD sends the start/stop messages and also periodic accounting messages.

Aruba recommends that you set up interim accounting because it provides important context to CPPM about the client's location and network usage. Admins can then view this information in Access Tracker. CPPM can also deliver this information to third-party devices integrated as endpoint context servers.

To enable interim accounting on IAPs, make sure to enable accounting in two locations. Enable it in the RADIUS server settings. Also enable accounting in the WLAN security settings. Choose to send accounting information to the authentication server defined for the WLAN. Then set the interval for the interim updates.

On AOS-CX switches, you enable interim accounting for authenticated clients with this command: **aaa accounting port-access start-stop interim <*minutes*> group <*group_name*>**

Standard Ports for Network Device and CPPM Communications



RADIUS

UDP 1812 (authentication)
UDP 1813 (accounting)
UDP 3799 (CoAs)

RadSec

TCP 2083

MOD 1- 54

If a firewall exists between NADs and CPPM, you must ensure that the firewall permits the required ports. When NADs and CPPM communicate with RADIUS, these ports must be open:

UDP 1812 for RADIUS authentication

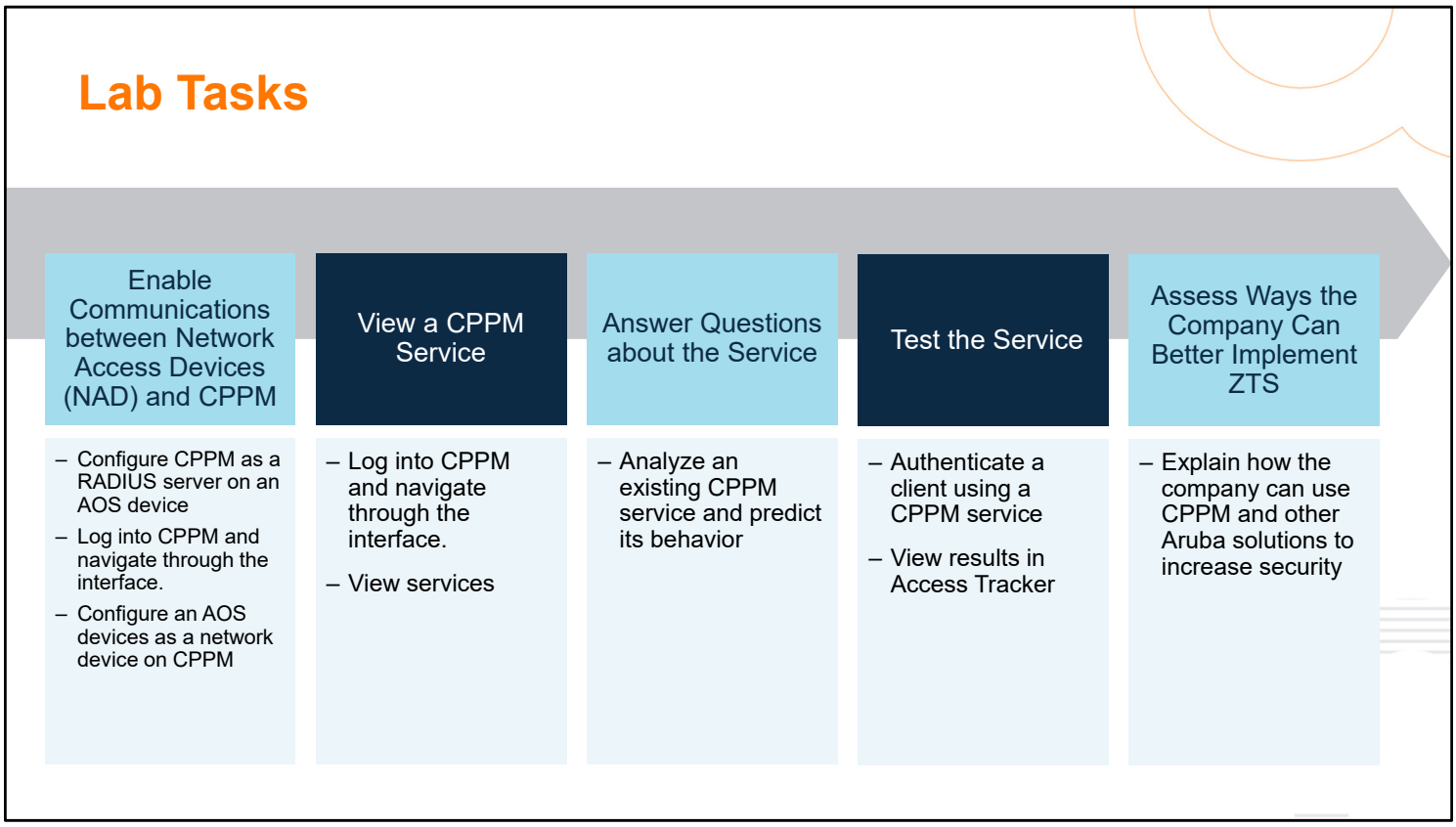
UDP 1813 for RADIUS accounting

UDP 3799 for CoAs

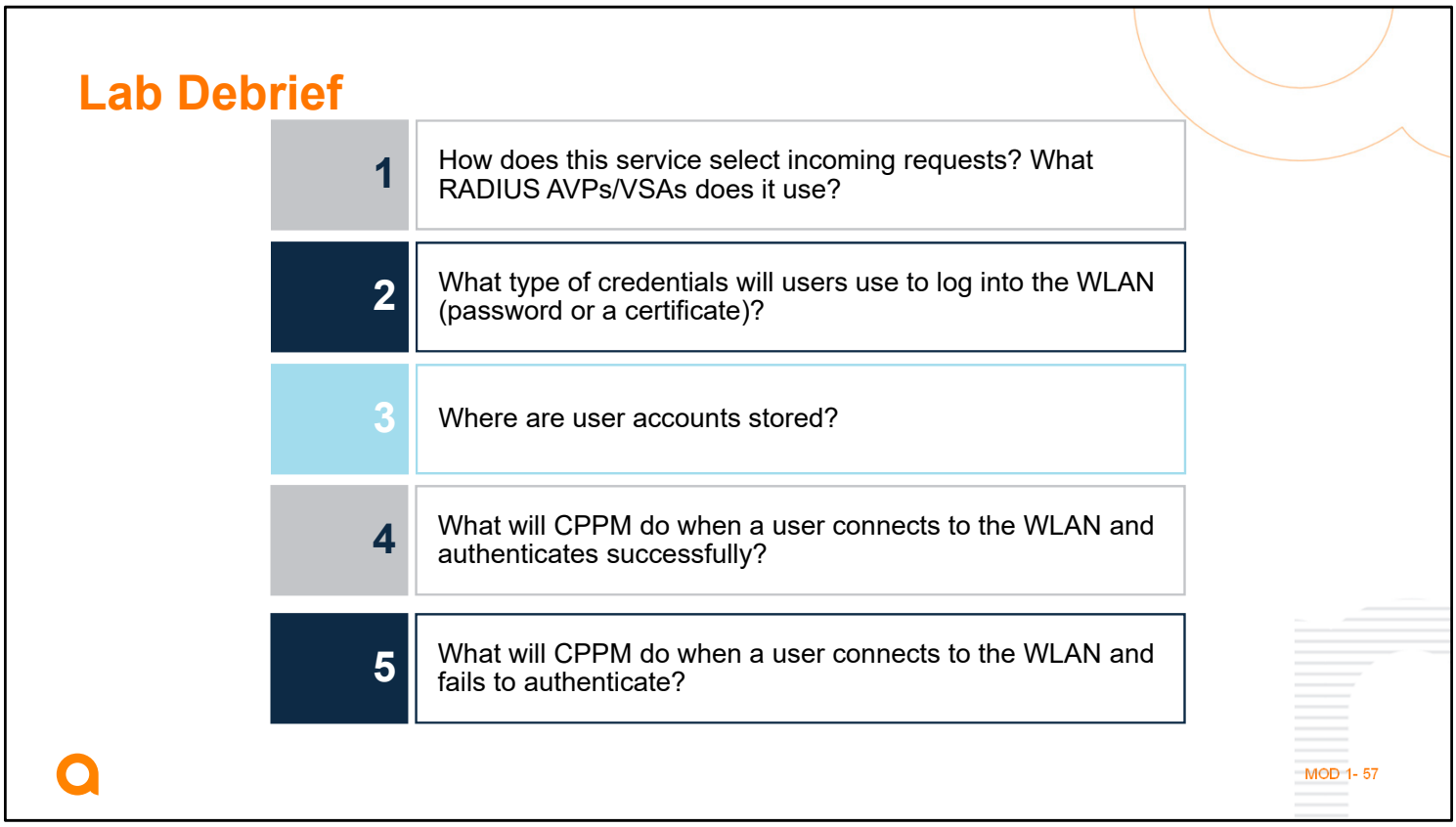
For RadSec, only one port is required: TCP 2083. The TCP session carries all RADIUS authentication, accounting, and CoA messages.

Note that these are the standard ports. If you change your configuration to use non-standard ports, the firewall must permit those instead.


Lab 1



You will now access a ClearPass server, which is already set up in your lab environment. You will log into CPPM and explore a service already configured on it. You will then test out authenticating clients to the network using this service, and you will see whether you correctly predicted the results. Finally, you will then suggest some concrete ways that the company can start to improve its security posture.



You analyzed an existing CPPM service during the lab. Discuss what you found with your classmates.

Answers are provided below:

How does this service select incoming requests? What RADIUS AVPs/VSAs does it use?

– It selects requests for wireless network access (RADIUS standard AVP NAS-Port-Type = Wireless (19) and RADIUS standard AVP Service-Type = Login-User (1), Framed-User (2), or Authenticate-Only (8). It further requires that the wireless authenticator sends an Aruba VSA indicating the SSID (Aruba-Essid-Name). This service only requires that this VSA exist, so it will match all Aruba mobility device requests for 802.1X authentication.

What type of credentials will users use to log into the WLAN (password or a certificate)?

– The Authentication method is PEAP. The Inner method supports MSCHAP, EAP-TLS, or EAP-GTC. This means that theoretically users could log in with usernames/passwords or certificates. However, PEAP is almost always used with MSCHAP and usernames/passwords.

Where are user accounts stored?

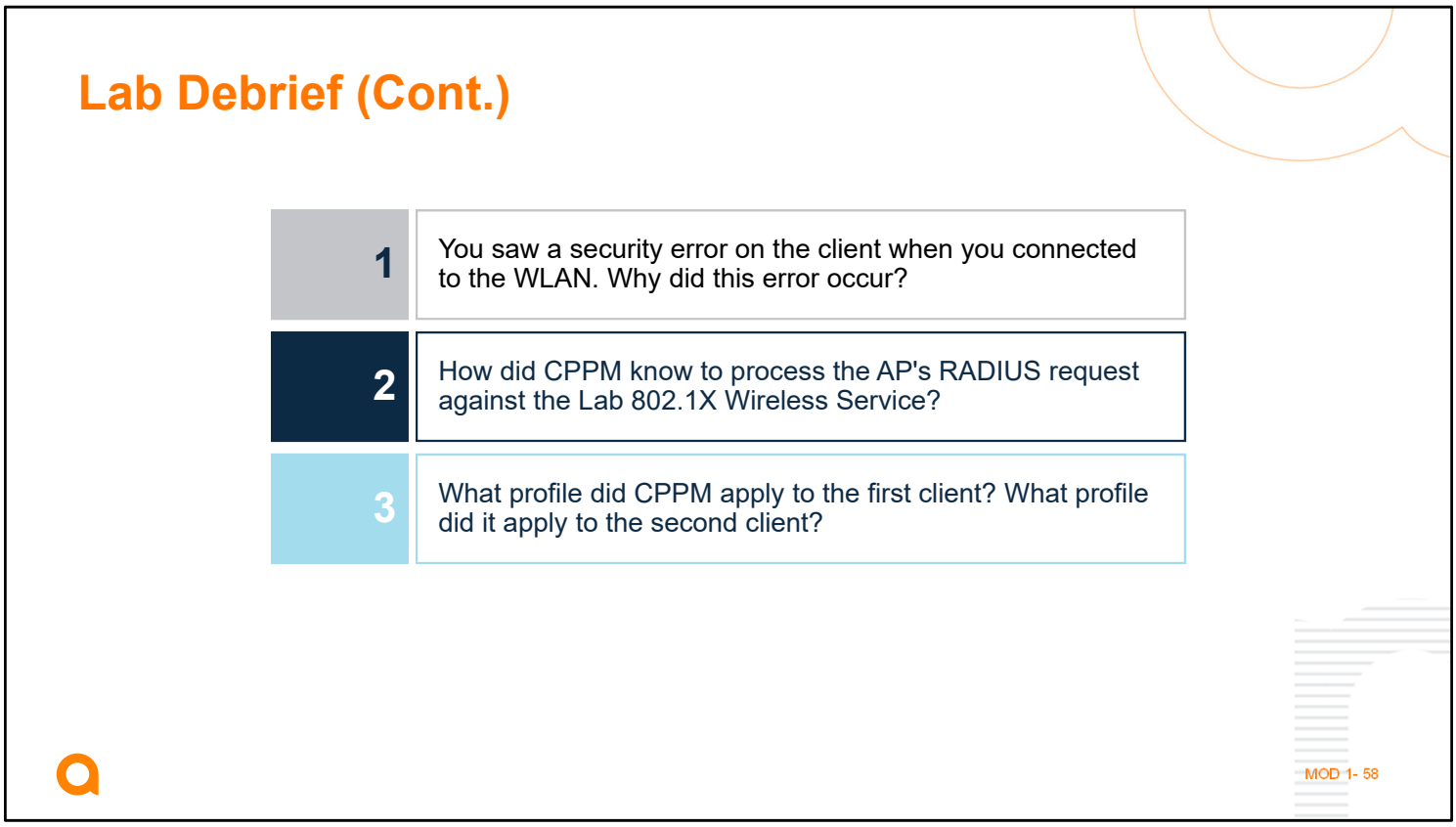
– The authentication source is an AD instance. Therefore, accounts are stored in AD.

What will CPPM do when a user connects to the WLAN and authenticates successfully?

– Based on the enforcement policy and the profile in its rule, CPPM will send an Access-Accept with no other attributes for customizing access.

What will CPPM do when a user connects to the WLAN and fails to authenticate?

– CPPM will send an Access-Reject.



Now discuss what you discovered when you connected clients to the WLAN.

Answers are provided below:

You saw a security error on the client when you connected to the WLAN. Why did this error occur?

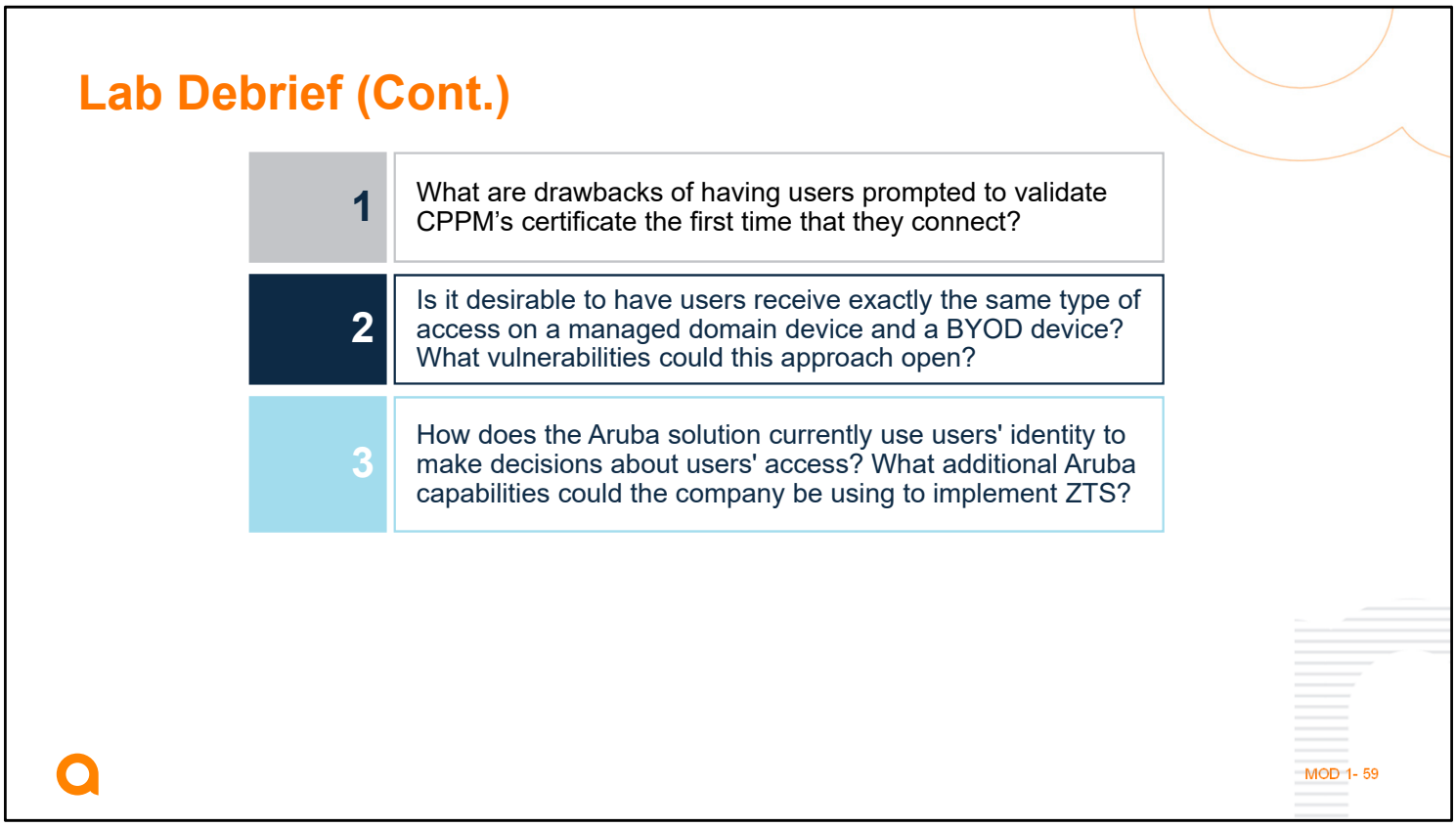
– As the RADIUS server, CPPM presents a certificate to authenticate itself to the client during 802.1X. The client has not been set up to trust this certificate.

How did CPPM know to process the AP's RADIUS request against the Lab 802.1X Wireless Service?

– As shown in Access Tracker, the AP’s RADIUS request includes several AVPs and VSAs. Among these are the three that match up with the ones specified in the lab 802.1X Wireless Service rules.

What profile did CPPM apply to the first client? What profile did it apply to the second client?

– One client is a domain computer, and the other is a BYOD device. The users on the clients are in different groups. But, based on the service, CPPM assigns the same profile to both: Allow Access Profile. This profile sends a simple Access-Accept with no extra AVPs or VSAs.



Now discuss the implications of what you explored. How can you change and build on the current solution to help the company move to a ZTS approach.

Answers are provided below:

What are drawbacks of having users prompted to validate CPPM's certificate the first time that they connect?

- Some users might choose not to trust the certificate, which will prevent them from connecting to the network. Most users will probably ignore the error, but even that is a problem. It is best practice to avoid situations in which users must choose to ignore a security error. Ignoring security errors gives users bad habits. Most users will not be able to tell the difference between the legitimate RADIUS server certificate and one presented by a rogue server (such as one in a rogue AP). And if users do authenticate to a rogue server, they might expose their credentials or fall prey to a MitM attack.

Is it desirable to have users receive exactly the same type of access on a managed domain device and a BYOD device? What vulnerabilities could this approach open?

- In most situations, these two types of devices should receive different levels of access. A device managed by the corporation is likely much more secure than a BYOD device, which might not have the proper firewall settings, antivirus software, and up-to-date patches. Because BYOD devices are more vulnerable to compromise, they should not have access to the most sensitive resources.

How does the Aruba solution currently use users' identity as it makes decisions about users' access? What additional Aruba capabilities could the company be using to implement ZTS?

- Currently the solution is only checking that the user is a valid member of the domain. However, the company has not set up the Aruba solution to take advantage of what it knows about users'

identities to grant them different levels of access. The company could benefit by assigning users to different roles based on factors such as group membership. CPPM can then communicate these roles to the infrastructure, which can then enforce different access control.

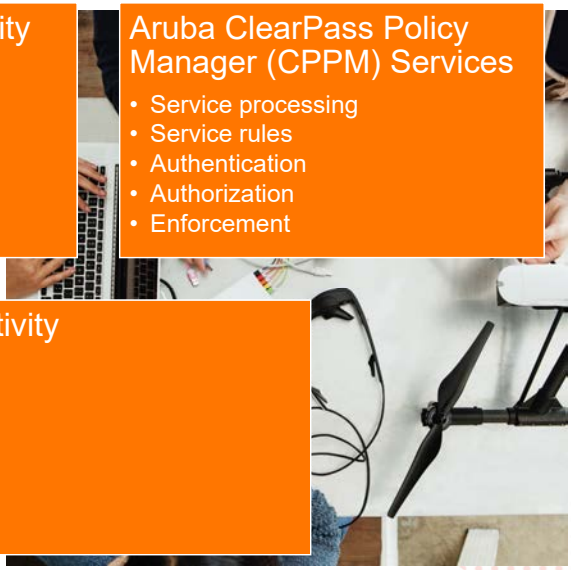
- The company could also add capabilities like ClearPass OnGuard to assess devices' security posture and only allow healthy devices full access to the network.
- And the company could be profiling devices and taking that information into account in policies too.

Summary

Zero Trust Security
- Internal threat vectors
- Zero Trust Security

Aruba Zero Trust Security
- Aruba ZTS
- Visibility
- Authentication
- Role-based access control
- Continuous monitoring & enforcement and response

Aruba ClearPass Policy Manager (CPPM) Services
- Service processing
- Service rules
- Authentication
- Authorization
- Enforcement



Aruba CPPM Network Devices
- What network device entries are required
- RADIUS vs RadSec
- Enabling CoAs

Lab Activity
- Lab 1

MOD 1- 60

Congratulations! You have completed the first module. You should now be able to explain why companies require a Zero Trust Security approach and how Aruba ESP provides superior ZTS. You also know the basics of setting up CPPM to act as the foundation for a ZTS solution.