CHAPTER 24

Security Configurations on DCNM-LAN Client

The Cisco NX-OS software supports security features that can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

This chapter includes the following sections:

- Configuring IP ACLs, page 24-1
- Configuring MAC ACLs, page 24-2
- Configuring VLAN ACLs, page 24-2
- Configuring ARP ACLs, page 24-2
- Configuring Object Groups, page 24-3
- Configuring AAA, page 24-3
- Configuring Time Ranges, page 24-3
- Configuring RADIUS, page 24-3
- Configuring TACACS+, page 24-4
- Configuring 802.1X, page 24-4
- Configuring User Accounts and RBAC, page 24-5

For detailed information about the security configuration on DCNM-LAn client, see Security Configuration Guide, Cisco DCNM for LAN, Release 7.x.

Configuring IP ACLs

You can configure an IP ACL on the device. An IP ACL is an ordered set of rules that you can use to filter traffic based on IPv4 or IPv6 information in the Layer 3 header of packets. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that an IP ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

Configuring MAC ACLs

You can configure a MAC ACL on the device. MAC ACLs are ACLs that filter traffic using the information in the Layer 2 header of each packet. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that a MAC ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

Configuring VLAN ACLs

A VLAN ACL (VACL) is one application of a MAC ACL or IP ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

Configuring ARP ACLs

You can configure an ARP ACL on the device. An ARP ACL is an ordered set of rules that you can use to filter ARP traffic for dynamic ARP inspection (DAI). Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that an ARP ACL applies to an ARP packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

When you configure the device to apply an ARP ACL to traffic, the ACL take precedence over entries in the DHCP snooping binding database. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Configuring Object Groups

An object group is a group of IP addresses or a group of TCP or UDP ports. When you create an access control list (ACL) rule, you can specify the object groups rather than specifying IP addresses or ports. Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules.

Configuring AAA

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure authentication, authorization, and accounting (AAA) on Cisco NX-OS devices.

You can configure authentication, authorization, and accounting (AAA) network security services to provide the primary framework through which you set up access control on your router or access server. Based on the user ID and password combination that you provide, the Cisco NX-OS device performs local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers.

Note System-message logging levels for AAA must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

Configuring Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the device determines that a particular ACL applies to traffic arriving on an interface, if a rule in the ACL uses a time range that is not in effect, the device does not compare the traffic to that rule.

IPv4, IPv6, and MAC ACLs support time ranges. When the device applies an ACL to traffic, the rules that are in effect are as follows:

- All rules that are not configured with a time range.
- Rules that are configured with a time range which is active at the second that the device applies the ACL to traffic.

The device supports named, reusable time ranges. This allows you to configure a time range once and specify it by name when configure many ACL rules.

Configuring RADIUS

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on NX-OS devices.

You can configure RADIUS on a device. The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco NX-OS devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

Note System-message logging levels for RADIUS must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

Configuring TACACS+

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

You can use TACACS+ to provide centralized validation of users attempting to gain access to a device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your device are available.

Note System-message logging levels for TACACS+ must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

Configuring 802.1X

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure IEEE 802.1X port-based authentication on Cisco NX-OS devices.

802.1X defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a device port.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Note System-message logging levels for 802.1X must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception.

For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

Configuring User Accounts and RBAC

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure user accounts and role-based access control (RBAC) on NX-OS devices.

You can create and manage users accounts and assign roles that limit access to operations on the NX-OS device. Role-based access control (RBAC) allows you to define the rules for an assign role that restrict the authorization that the user must have to access management operations.