Cisco Nexus 7000 Security Features

Comprehensive and Practical for the Data Centers

Comprehensive Security for the Data Center Network

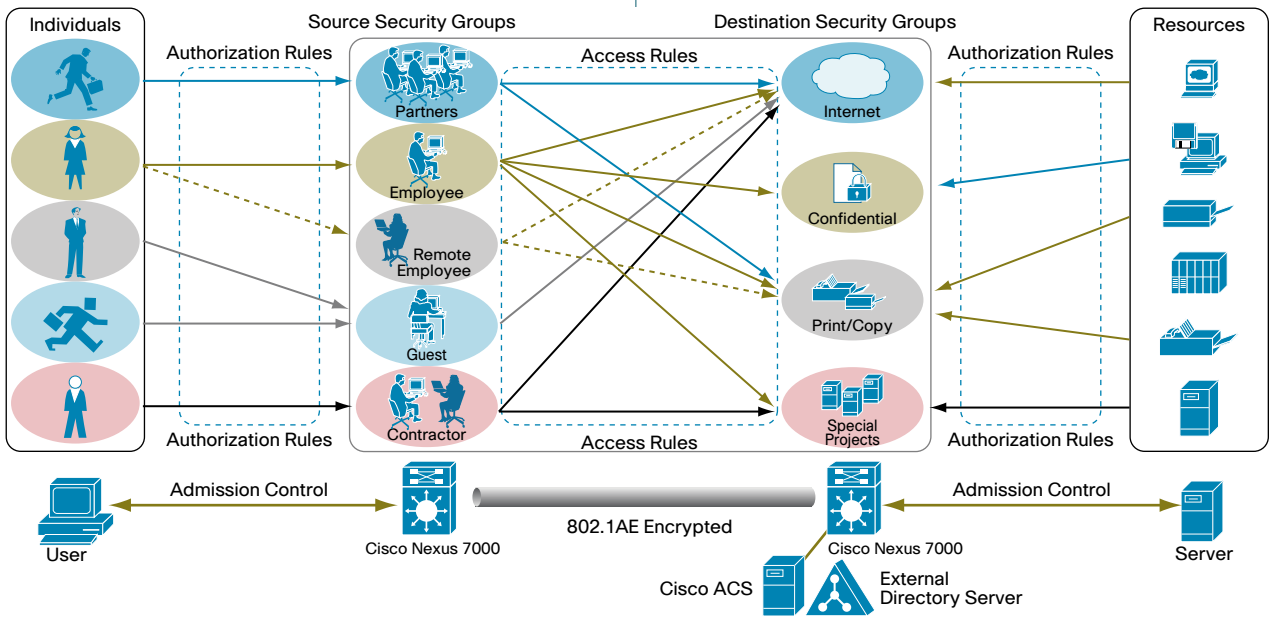
Data centers in enterprises store confidential information about employees, customers, and external stakeholders as well as assets such as intellectual property and critical business information. Users, internal and external, access corporate data from a variety of devices and access points. Securing the data infrastructure, complying with regulators and protecting data-in-transit as well as data-at-rest is a network administration as well as technology challenge. Protecting the data center requires an integrated policy at all levels, from the network infrastructure to the computing applications. A secure network fabric goes a long way toward protecting the corporate data center. Cisco Nexus 7000 series is designed to address the infrastructure security needs for next generation data centers.

The Cisco® Nexus 7000 Series is a highly scalable end-to-end 10 Gigabit Ethernet switch series for mission-critical data center operations. The fabric architecture scales beyond 15 terabits per second (Tbps), with future support for 40-Gbps and 100-Gbps Ethernet. Powered by Cisco NX-OS, a state-of-the-art modular operating system, the platform is designed for exceptional scalability, continuous system operation, serviceability, and transport flexibility. The Cisco Nexus 7000 Series provides comprehensive security features supported by a robust control plane and wire-rate encryption and decryption, allowing security controls that are less complex and more transparent to the protocols and applications in the data center. It supports Cisco TrustSec, a new architecture from Cisco for a converged policy framework to create role-aware networks and pervasive integrity and confidentiality.

Cisco Nexus 7000 Series Data Center Security Support

- Cisco TrustSec, offered through distinct built-in hardware and software features, providing device admission control, security group–based policies, and link-layer cryptography
- Integrated Security Features to protect the data center network and devices from DoS attacks, network host spoofing or snooping of data and voice traffic
- IEEE 802.1x for authentication and authorization
- Port access control lists (PACLs), Router ACLs (RACLs), VLAN ACLs (VACLs), and Role-based access control (RBAC) for securing privileges and providing flexibility in protecting information
- Control Plane Protection with enhanced hardware based policing

Figure 1. Cisco TrustSec in the Data Center



Cisco TrustSec

Cisco TrustSec is a new rich policy-based service for admission and access control, with packet confidentiality and integrity built into the network fabric. Cisco TrustSec uses security group tags (SGTs) based on the IEEE 802.1AE standard to create role-aware networks where role information is available at every enforcement point in the network. (Figure 1) Specific components in Cisco Nexus 7000 include:

Admission control: The Cisco Nexus 7000 Series has built-in features to communicate with an authentication, authorization, and accounting (AAA) or RADIUS server and provide comprehensive yet unified policy to authenticate and authorize network devices and endpoints.

- Network Device Admission Control (NDAC) to authenticate all network devices
- Endpoint Admission Control (EAC) to authenticate access devices and download authorization policies per user or device port

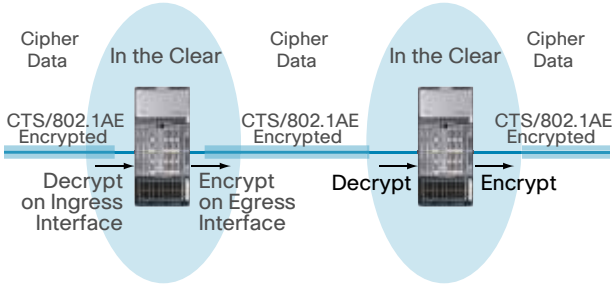
Cisco Nexus 7000 Security Features

Comprehensive and Practical for the Data Centers

At-A-Glance

- LinkSec (IEEE 802.1AE): Wire-rate link-layer cryptography is provided at all ports. Packets are encrypted on egress and decrypted on ingress so they are clear inside the device. This approach allows insertion of network services that operate on non-encrypted traffic, while still guaranteeing the integrity and privacy of the traffic as it transits the wire (Figure 2).

Figure 2. Packet Confidentiality and Integrity (IEEE 802.1AE)



- Security Group ACLs (SGACLs): This scalable and topology-independent access control mechanism is unlike traditional ACLs. SGACLs group users based on similar privileges by using specific security group tags (SGTs). Because policies are based on SGTs rather than IP addresses users and resources can be mobile without losing their security privileges.

Authentication and Authorization

To protect the data center from unauthorized users, the Cisco Nexus 7000 Series supports multiple authentication mechanisms, such as IEEE 802.1x, MAC-Auth-Bypass (MAB). Authorization can be enforced through ACLs, VLAN assignment, or Cisco TrustSec policies. IEEE 802.1x along with RADIUS is used for transporting authentication and authorization information. MAB allows MAC-address-based authentication, and IEEE 802.1x provides credential-based identity verification.

Operationally, different levels of management access can be granted to the Cisco Nexus 7000 Series Switches. RBAC allows the definition and enforcement of multiple levels of access rights to the management plane.

Integrated Security Features

Cisco NX-OS supports Integrated Security which includes comprehensive features to protect the data center from denial of service (DoS) attacks, rogue DHCP servers and man-in-the-middle attacks. Highlighted features are:

- Unicast Reverse Path Forwarding (uRPF): Protects the network by denying access to traffic with spoofed IP addresses and tracing the traffic to its correct source. Cisco Nexus 7000 Series has built-in hardware features to perform multipath uRPF checks for up to16 paths for the same source network.
- Packet Broadcast Suppression: This feature protects the data center against broadcast storms at the port level that pose risks to bandwidth availability.
- Packet Sanity Checks: Cisco Nexus 7000 Series forwarding engine performs extensive checks on IPv4 and IPv6 packet headers to protect the network from illegal packets.
- IP Source Guard: Cisco Nexus 7000 Series supports an efficient hardware based implementation of this feature that filters source IP addresses and prevents impersonation by malicious hosts.
- Dynamic ARP Inspection (DAI): To prevent ARP spoofing (man-in-the-middle attacks) and ARP cache poisoning, Cisco NX-OS uses DAI to validate IP-to-MAC address bindings in the ARP packets, logging and discarding packets that fail the check.
- Port Security: To protect the Layer-2 content-addressable memory (CAM) tables from attacks (flooding, MACaddress spoofing), Cisco NX-OS supports port security to control the port access.

Enhanced Control Plan Protection

Control Plane Policing (CoPP): This set of hardware-based features in the Cisco Nexus 7000 Series protects the supervisor from DoS attacks preventing outages that can affect business. Enhanced CoPP provides both broad and granular controls over the traffic that reaches the supervisor CPU such as layer 2 broadcasts and irrelevant traffic redirections.

Access Control Lists Enhancement

Cisco NX-OS supports RACLs, VACLs, and PACLs as well as Policy Based Routing (PBR) by matching Layer 2, 3, and 4 header fields. With PBR, the packet can be forwarded to the next hop based on administrative policy instead of a routing metric, allowing flexibility and load sharing across the data center. Cisco Nexus 7000 Series hardware supports a new unique ACL programming paradigm—Atomic ACLs allow reconfiguration of ACLs without disrupting traffic. For security ACLs and quality-of-service (QoS) policies, Cisco NX-OS supports a dry-run configuration session, where the user can verify the setup against available systems resources before committing. Selective programming also promotes scalability, usability, and better manageability in the data center.

Why invest in security for the data center?

With the Cisco Nexus 7000 switch, security in the data center is easy to deploy and reduces operational expenses.

- Role-based access control reduces costs and complexity
- Comprehensive security with a robust control plane
- Packet confidentiality and Integrity with multiple integrated features for a secure data center

For More Information

- Cisco Nexus 7000 Series: http://www.cisco.com/go/nexus7000
- Cisco NX-OS: http://www.cisco.com/go/nxos