CHAPTER 3

Enterprise Core

The core is the piece of the network infrastructure that glues all the other modules together. The core is a high-speed infrastructure whose objective is to provide a reliable and scalable Layer-2/Layer-3 transport. It routes and switches traffic as fast as possible from one network module to another such as campuses, data center, WAN edge, and Internet edge.

The core network is not expected to provide end customer services by itself. Rather, it is a building block used to enable other modules within the network to provide these services to the end devices. External IP traffic is never destined to the core network infrastructure. Generally, the only packets destined to these devices are internal control and management traffic generated by other network elements or management stations within the same administrative domain.

Key Threats in the Core

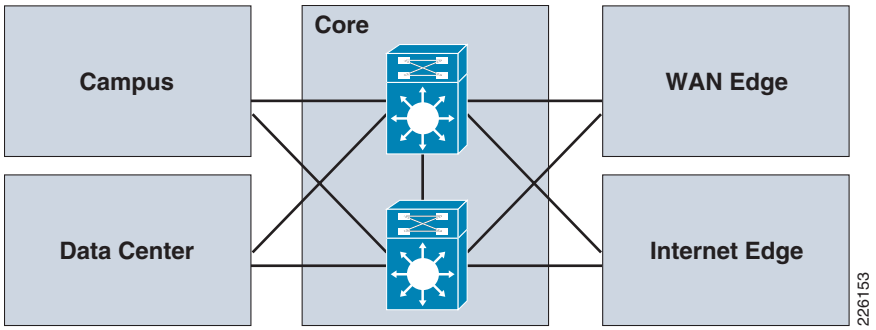
The following are some of the threat vectors affecting the enterprise core:

- Service disruption—DoS and DDoS attacks on the infrastructure.
- Unauthorized access—Intrusions, unauthorized users, escalation of privileges, unauthorized access to restricted infrastructure, and routing protocol attacks.
- Data disclosure and modification—Packet sniffing, man-in-the-middle (MITM) attacks of data while in transit.

Enterprise Core Design

The core module in the SAFE architecture is nearly identical to the core module of any other network architecture. Standard implementation guidelines were followed in accordance with the core, distribution, and access layer deployments commonly seen in well-designed Cisco-based networks. It is implemented with redundant switches that aggregate the connections from the various places in the network (PINs) such as campuses, data centers, WAN edge, and Internet edge as shown in Figure 3-1.

Figure 3-1 Enterprise Core Topology



Design Guidelines for the Core

The primary role of security in the enterprise core module is to protect the core itself, not to apply policy to mitigate transit threats traversing through the core. Such threats should be filtered at the network edge or within other network modules to mitigate transit attack traffic from adversely affecting authorized transit traffic. A well designed network edge security policy will greatly limit the exposure of the network core to attacks. However, human error, misconfiguration, change management, and exception cases dictate that core security mechanisms must be defined and deployed in support of the defense-in-depth principles. These core policies help to mitigate the risk to the core if edge policies are inadvertently bypassed.

Effective core security demands the implementation of various security measures in a layered approach and guided under a common strategy. These measures include enabling security at the edge and within the networks connecting to the core and securing the core switches themselves. The core switches are secured following the infrastructure baseline security principles explained in Chapter 2, "Network Foundation Protection." This includes restricting and controlling administrative device access, securing the routing infrastructure, and protecting the management and control planes.

For complete details on implementing and monitoring infrastructure baseline security best practices including configuration examples, refer to Chapter 2, "Network Foundation Protection." The following summarizes the baseline security best practices specific to securing the enterprise core infrastructure. It lists techniques for securing the control and management planes providing a strong foundation on which more advanced methods and techniques can subsequently be built on.

The following are the key areas of the Network Foundation Protection (NFP) baseline security best practices applicable to securing the enterprise core:

- Infrastructure device access—Implement dedicated management interfaces to the out-of-band (OOB) management network[1], limit the accessible ports and restrict the permitted communicators and the permitted methods of access, present legal notification, authenticate and authorize access using AAA, log and account for all access, and protect locally stored sensitive data (such as local passwords) from viewing and copying.
- Routing infrastructure—Authenticate routing neighbors, implement route filtering, use default passive interfaces, and log neighbor changes.
- Device resiliency and survivability—Disable unnecessary services, filter and rate-limit control-plane traffic, and implement redundancy.

1. For more information on implementing an OOB management network, refer to Chapter 9, "Management."

- Network telemetry—Implement NTP to synchronize time to the same network clock; maintain device global and interface traffic statistics; maintain system status information (memory, CPU, and process); and log and collect system status, traffic statistics, and device access information.

Threats Mitigated in the Core

Table 3-1 summarizes the techniques used by the SAFE architecture design to mitigate threats to the enterprise core infrastructure.

Table 3-1 Core Threat Mitigation Features

	DoS on Infrastructure	DDoS on Infrastructure	Unauthorized Access	Intrusions	Routing Protocol Attacks	Botnets	Visibility	Control
System and Topological Redundancy	Yes	Yes			Yes	Yes		Yes
Disabling Unneeded Services	Yes	Yes	Yes	Yes			Yes	Yes
Strong Password Policy			Yes	Yes				Yes
AAA			Yes	Yes			Yes	Yes
SSH			Yes	Yes				Yes
SNMP Authentication			Yes	Yes			Yes	Yes
Session ACLs	Yes	Yes	Yes	Yes			Yes	Yes
Router Neighbor Authentication	Yes		Yes		Yes			Yes
CoPP	Yes	Yes	Yes	Yes	Yes	Yes		Yes
NetFlow, Syslog							Yes	