



# ISC Security Concepts

This chapter contains the following sections:

- [ISC Security Management, page 1-1](#)
- [Site-to-Site VPN Concepts, page 1-3](#)
- [Remote Access VPN Concepts, page 1-3](#)
- [NAT Concepts, page 1-3](#)
- [Firewall Concepts, page 1-4](#)
- [Device Interfaces, page 1-4](#)

## ISC Security Management

Cisco ISC 3.0 Security Management enables customers to manage their network security from a single, global application.

The main services for ISC 3.0 Security Management are site-to-site VPN, remote access VPN, NAT, firewall, and network-based VPN. Site-to-site VPN, remote access VPN, NAT, and firewall are all described in this guide. Network-based VPN is described in the *Cisco IP Solution Guide, 3.0: MPLS VPN Management User Guide*.

**Table 1-1 IP Solution Center Security Management Features**

Service	Features Supported
Site-to-Site VPN	<ul style="list-style-type: none"> <li>• Pure IPsec for Cisco IOS Software, PIX Firewall, and VPN 3000</li> <li>• IPsec + GRE for Cisco IOS and PIX Firewall Software</li> <li>• DMVPN for Cisco IOS Software</li> <li>• Easy VPN for Cisco IOS Software</li> </ul>
Remote Access VPN	<ul style="list-style-type: none"> <li>• Remote Access VPNs on Cisco IOS devices, PIX Firewalls, and VPN 3000 devices</li> </ul>
NAT	<ul style="list-style-type: none"> <li>• Static translations including network, host, or port-based translations</li> <li>• Dynamic translations including NAT and PAT</li> <li>• Overlapping IP address spaces</li> </ul>

**Table 1-1 IP Solution Center Security Management Features (continued)**

Service	Features Supported
Firewall	<ul style="list-style-type: none"> <li>• Access rules</li> <li>• Inspection rules</li> <li>• URL filtering using N2H2 or Websense</li> <li>• Exclusive domain URL filtering using Cisco IOS Software</li> </ul>
Network-Based VPN	Network-based is covered in the <i>Cisco IP Solution Guide, 3.0: MPLS VPN Management User Guide</i> ; please refer to the <i>Cisco IP Solution Guide, 3.0: MPLS VPN Management User Guide</i> for information on IPsec-to-MPLS service mapping.
Provisioning Templates	<ul style="list-style-type: none"> <li>• IDS (Cisco IOS devices only)</li> <li>• Certificate enrollment and verification</li> <li>• Additional VPN 3000 features</li> <li>• User-definable template option for specialized services or configurations</li> </ul>

For site-to-site VPN, remote access, and firewall services, you create security policies to then use in ISC service requests. For site-to-site VPN, remote access, NAT, and firewall services, you create a service request, which bundles together the service policy (as applicable) and the list of CPE devices for which they are intended. You then deploy the service request, which creates the device-level configurations (called *configlets*) and pushes them down to provision all security devices in your network at the same time.

Furthermore, once the security policies are defined, they can be reused across multiple networks in multiple service requests. Service requests can be validated by checking the service request state and through service request audits.

All policies and service requests are entered through the ISC graphical user interface (GUI).

While deploying a service request, ISC attempts to upload the current configuration file of each network device, referred to as *CPE device*. It then generates the configlet containing the commands necessary to enable the service, such as the crypto maps, transform sets, IKE policies, and access control lists (ACLs). Additional commands are also included in the configlet, such as firewall rules (ACLs and inspection rules) and NAT mappings.

ISC then downloads the service request configlets to the CPE devices. (ISC supports a number of transport mechanisms while communicating with CPE devices, such as SSH, Telnet, or CNS.) Upon completion of the download, the service is operational.

The user may then schedule a one-time or regular task to audit the service. (Auditing is uploading the current configuration file of the CPE devices and ensuring they contain all the necessary service-configuration commands.) If some commands are missing, an audit report is generated indicating the missing commands. If this occurs, you can re-deploy the service request to correct the configuration or deploy a new service request to change the configuration.

## Site-to-Site VPN Concepts

Site-to-site VPNs provide secure network traffic between customer sites, usually in different geographic areas. For this reason, who owns the site (the site ownership), the grouping of devices in the site, and the configuration of individual devices are all important to provisioning site-to-site VPNs. ISC site-to-site VPN services use all of this information, combined with the IPsec parameters you specify, to provision a site-to-site VPN.

Specifically, ISC site-to-site VPNs are implemented through policy creation and service request deployment. In the site-to-site policy, you define the IPsec parameters that create the VPN tunnel and describe the network topology (either full mesh or hub-and-spoke). When you create the service request, you define what traffic should be sent through the VPN tunnel and what traffic should not. Once created, you can provision multiple CPE devices using the same policy in one or more service requests.

## Remote Access VPN Concepts

Remote access VPNs connect telecommuters and mobile users to corporate networks through secure IPsec tunnels.

Remote workers and users use a variety of technologies to access these corporate networks, such as dial-up, broadband over cable, digital subscriber line (DSL), and wireless. What they have in common is that a VPN client resides on the user's workstation and that client initiates the VPN tunnel. At the other end of the VPN tunnel is the VPN headend, a CPE device at the edge of the corporate site. In other words, the main components of a remote access VPN are a VPN client and a VPN headend device (or VPN gateway).

When the VPN client initiates a connection with a VPN headend device, the negotiation consists of device authentication through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (XAuth). Then the group profile is pushed down using Mode Configuration, and an IPsec security association (SA) is created to complete the VPN connection. An ISC remote access policy defines the IPsec parameters that the VPN client and VPN headend use to create the VPN tunnel, and ISC provisions devices in the network through an ISC service request.

## NAT Concepts

Network Address Translation (NAT) is designed for IP address simplification and conservation by enabling private IP internetworks to use non-registered IP addresses to connect to the Internet. NAT operates on a router or firewall, usually connecting a network site to the Internet, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. As part of this functionality, NAT can be configured to advertise only one address for the entire network to the outside world. This hides internal network addresses from the outside world.

Unlike other ISC security services, NAT uses only a service request. There is no policy creation step needed for NAT services. Deployment of a NAT service request, using ISC, creates and delivers configuration to the target devices, audits the device configuration, and maintains it for the service life cycle.

# Firewall Concepts

Firewalls are devices that monitor and filter network traffic, and control access to network assets based on packet inspection. Firewalls are often placed between a private network and an external network such as the Internet. (With a firewall between your network and the Internet, all traffic coming from the Internet must pass through the firewall before entering your network.)

Firewalls are usually positioned at the entrance points of your network, but they can also be deployed between segments within your network. For example, you can position firewalls at all the entry points into a research and development network to prevent unauthorized access to proprietary information. In any case, if your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

ISC supports firewall services that include traffic filtering, inspection rules, and URL filtering. To provision firewall services using ISC, you must first define the firewall policy. After creating the firewall policy you can then apply it to multiple Cisco firewall devices through an ISC service request.

## Device Interfaces

When you add devices to your network, you must designate the device interface roles. Security provisioning uses the designated interface roles to configure security services.

Site-to-site and remote access VPNs use the concepts of *public* (outside) interfaces and *private* (inside) interfaces. Interfaces on which VPN tunnels terminate are known as the public interfaces, and interfaces behind which the customer subnets reside are known as the private interfaces.

Because they often may have multiple interfaces, firewalls are flexible in how you can define interface relationships. Their interfaces may be public to part of one network and private to another part of the same network or another network. Consequently, the convention is for firewalls to use *outside*, *inside*, *dmz*, and user-defined interface names. *Outside* is generally used in the same sense as public for VPN interfaces, and *inside* is generally used in the same sense as private for VPN interfaces. The designation *dmz*, for demilitarized zone, is often used for firewall interfaces that separate areas within a corporate network.

NAT also uses the outside and inside interface naming convention. For NAT, the outside interface often connects to the Internet or a corporate network segment, and the inside interface often connects to an internal network or a network area for which addresses need to be conserved.

You can set the interfaces for a device either through **Service Inventory > Inventory and Connection Manager > Devices** (for individual devices) or when you use **Inventory Manager**. For information on how to setup individual devices or use **Inventory Manager**, please refer to the *Cisco IP Solution Center: Infrastructure Reference, 3.0*.