Configuring Security Features

This chapter describes how to configure security features on a Cisco 900 Series Integrated Services Routers (ISRs). This chapter contains the following sections:

Authentication, Authorization, and Accounting

Authentication, Authorization, and Accounting (AAA) network security services provide the primary framework through which you set up access control on your router. Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you choose, encryption. Authorization provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet. Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

AAA uses protocols such as Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), or Kerberos to administer its security functions. If your router is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

For information about configuring AAA services and supported security protocols, authentication authorization, accounting, RADIUS, TACACS+, or Kerberos, see the following sections of *Cisco IOS Security Configuration Guide: Securing User Services* at:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-mt/secuser-15-mt-library.html

- Configuring Authentication
- Configuring Authorization
- Configuring Accounting
- Configuring RADIUS
- Configuring TACACS+
- Configuring Kerberos

Configuring AutoSecure

The AutoSecure feature disables common IP services that can be exploited for network attacks and enables IP services and features that can aid in the defense of a network when under attack. These IP services are all disabled and enabled simultaneously with a single command, greatly simplifying security configuration on your router. For a complete description of the AutoSecure feature, see the feature document at:
https://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/convert/user_security/sec_autosecure.html

Configuring Access Lists

Access lists permit or deny network traffic over an interface, based on source IP address, destination IP address, or protocol. Access lists are configured as standard or extended. A standard access list either permits or denies passage of packets from a designated source. An extended access list allows designation of both the destination and the source, and it allows designation of individual protocols to be permitted or denied passage.

For more complete information on creating access lists, see the *Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T* at:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book.html.

An access list is a series of commands with a common tag to bind them together. The tag is either a number or a name. Table 8-1 lists the commands used to configure access lists.

Table 8-1 Access List Configuration Commands

Access Control List (ACL) Type	Configuration Commands
Numbered	
Standard	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
Extended	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]

Table 8-1 Access List Configuration Commands (continued)

Access Control List (ACL) Type	Configuration Commands
Named	
Standard	**ip access-list standard** *name* **deny** {*source* | *source-wildcard* | **any**}
Extended	**ip access-list extended** *name* **{permit | deny}** *protocol* {*source-addr* [*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

Access Groups

An access group is a sequence of access list definitions bound together with a common name or number. An access group is enabled for an interface during interface configuration. Use the following guidelines when creating access groups:

- The order of access list definitions is significant. A packet is compared against the first access list in the sequence. If there is no match (that is, if neither a permit nor a deny occurs), the packet is compared with the next access list, and so on.
- All parameters must match the access list before the packet is permitted or denied.
- There is an implicit "deny all" at the end of all sequences.

For information on configuring and managing access groups, see the "Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values" section of the *Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T* at:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book.html

Configuring Cisco IOS Firewall

The Cisco IOS Firewall lets you configure a stateful firewall where packets are inspected internally and the state of network connections is monitored. Stateful firewall is superior to static access lists because access lists can only permit or deny traffic based on individual packets, not based on streams of packets. Also, because the Cisco IOS Firewall inspects the packets, decisions to permit or deny traffic can be made by examining application layer data, which static access lists cannot examine.

To configure a Cisco IOS Firewall, specify which protocols to examine by using the following command in interface configuration mode:

ip inspect name *inspection-name protocol* **timeout** *seconds*

When inspection detects that the specified protocol is passing through the firewall, a dynamic access list is created to allow the passage of return traffic. The timeout parameter specifies the length of time that the dynamic access list remains active without return traffic passing through the router. When the timeout value is reached, the dynamic access list is removed, and subsequent packets (possibly valid ones) are not permitted.

Use the same inspection name in multiple statements to group them into one set of rules. This set of rules can be activated elsewhere in the configuration by using the **ip inspect inspection-name { in | out }** command when you configure an interface at the firewall.

For additional information about configuring a Cisco IOS Firewall, see *Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T* at:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

The Cisco IOS Firewall may also be configured to provide voice security in Session Initiated Protocol (SIP) applications. SIP inspection provides basic inspection functionality (SIP packet inspection and detection of pinhole openings), as well protocol conformance and application security. For more information, see *Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T* at:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/fw-sip-alg-aic.html

Zone-Based Policy Firewall

The Cisco IOS Zone-Based Policy Firewall can be used to deploy security policies by assigning interfaces to different zones and configuring a policy to inspect the traffic moving between these zones. The policy specifies a set of actions to be applied on the defined traffic class.

For additional information about configuring zone-based policy firewall, see the *Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T "* at:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

Configuring Cisco IOS IPS

Cisco IOS Intrusion Prevention System (IPS) technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IPS identifies attacks using "signatures" to detect patterns of misuse in network traffic. Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match currently active (loaded) attack signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised, it logs the event, and, depending on the action(s) configured to be taken for the detected signature(s), it does one of the following:

- Sends an alarm in syslog format or logs an alarm in Secure Device Event Exchange (SDEE) format
- Drops suspicious packets
- Resets the connection
- Denies traffic from the source IP address of the attacker for a specified amount of time
- Denies traffic on theconnection for which the signature was seen for a specified amount of time

For additional information about configuring Cisco IOS IPS, see the "Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements" section of

Cisco IOS Intrusion Prevention System Configuration Guide, Cisco IOS Release 15MT at:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_ios_ips/configuration/15-mt/sec-data-ios-ips-15-mt-book/sec-ips5-sig-fs-ue.html.

Content Filtering

Cisco 900 series ISRs provide category-based URL filtering. The user provisions URL filtering on the ISR by selecting categories of websites to be permitted or blocked. An external server, maintained by a third party, is used to check for URLs in each category. Permit and deny policies are maintained on the ISR. The service is subscription based, and the URLs in each category are maintained by the third party vendor.

For additional information about configuring URL filtering, see "Subscription-based Cisco IOS Content Filtering" at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/subscrip-cont-filter.html.

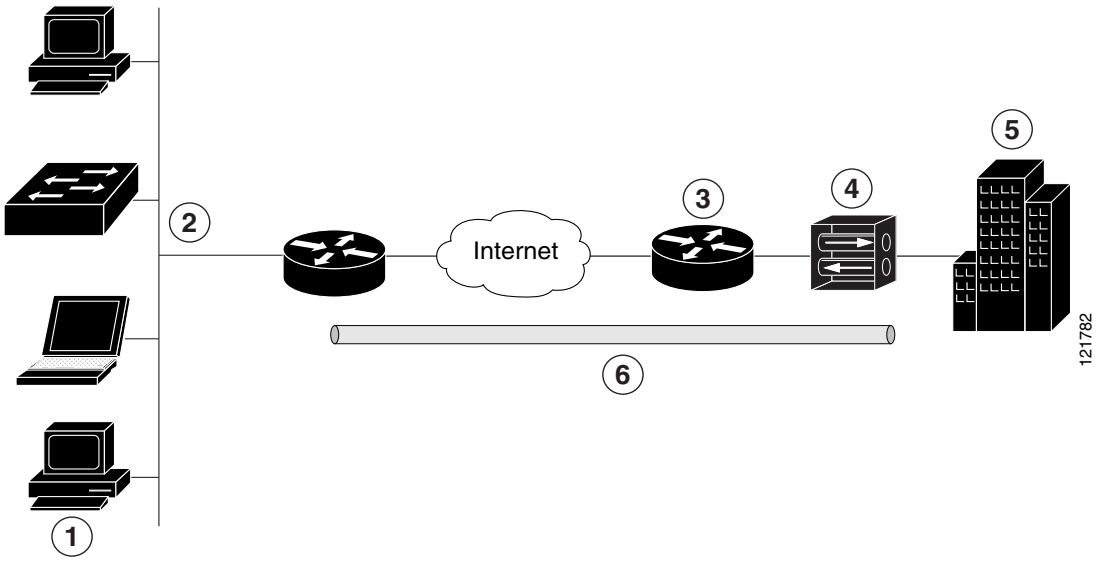
Configuring VPN

A Virtual Private Network (VPN) connection provides a secure connection between two networks over a public network such as the Internet. Cisco 900 series ISRs support two types of VPNs: site-to-site and remote access. Remote access VPNs are used by remote clients to log in to a corporate network. Site-to-site VPNs connect branch offices to corporate offices. This section gives an example for each.

Remote Access VPN Example

The configuration of a remote access VPN uses Cisco Easy VPN and an IP Security (IPSec) tunnel to configure and secure the connection between the remote client and the corporate network. Figure 8-1 shows a typical deployment scenario.

Figure 8-1 Remote Access VPN Using IPSec Tunnel



1	Remote networked users
2	VPN client—Cisco 900 series ISR
3	Router—Provides corporate office network access

4	VPN server—Easy VPN server; for example, a Cisco VPN 3000 concentrator with outside interface address 210.110.101.1
5	Corporate office with a network address of 10.1.1.1
6	IPSec tunnel

The Cisco Easy VPN client feature eliminates much of the tedious configuration work by implementing the Cisco Unity Client protocol. This protocol allows most VPN parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, Windows Internet Naming Service (WINS) server addresses, and split-tunneling flags, to be defined at a VPN server, such as a Cisco VPN 3000 series concentrator that is acting as an IPSec server.

A Cisco Easy VPN server–enabled device can terminate VPN tunnels initiated by mobile and remote workers who are running Cisco Easy VPN Remote software on PCs. Cisco Easy VPN server–enabled devices allow remote routers to act as Cisco Easy VPN Remote nodes.

The Cisco Easy VPN client feature can be configured in one of two modes—client mode or network extension mode. Client mode is the default configuration and allows only devices at the client site to access resources at the central site. Resources at the client site are unavailable to the central site. Network extension mode allows users at the central site (where the Cisco VPN 3000 series concentrator is located) to access network resources on the client site.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPSec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

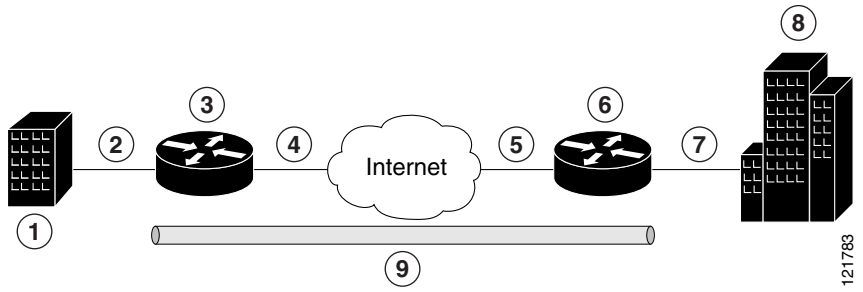
Cisco900 series ISRs can be also configured to act as Cisco Easy VPN servers, letting authorized Cisco Easy VPN clients establish dynamic VPN tunnels to the connected network. For information on configuring Cisco Easy VPN servers, see the *Easy VPN Server* feature at:

https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/convert/sec_easy_vpn_15_1_book.html

Site-to-Site VPN Example

The configuration of a site-to-site VPN uses IPSec and the generic routing encapsulation (GRE) protocol to secure the connection between the branch office and the corporate network. Figure 8-2 shows a typical deployment scenario.

Figure 8-2 Site-to-Site VPN Using an IPSec Tunnel and GRE



1	Branch office containing multiple LANs and VLANs
2	Fast Ethernet LAN interface—With address 192.165.0.0/16 (also the inside interface for NAT)
3	VPN client—Cisco 900 series ISR
4	Fast Ethernet or ATM interface—With address 200.1.1.1 (also the outside interface for NAT)
5	LAN interface—Connects to the Internet; with outside interface address of 210.110.101.1
6	VPN client—Another router, which controls access to the corporate network
7	LAN interface—Connects to the corporate network; with inside interface address of 10.1.1.1
8	Corporate office network
9	IPSec tunnel with GRE

For more information about IPSec and GRE configuration, see the Configuring Security for VPNs with IPSec" chapter of *Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15M&T* at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book.html.

Configuring Dynamic Multipoint VPN

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPsec) VPNs by combining GRE tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

For additional information about configuring DMVPN, see *Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T* at:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html

Configuring Group Encrypted Transport VPN

Group Encrypted Transport (GET) VPN is a set of features that are necessary to secure IP multicast group traffic or unicast traffic over a private WAN that originates on or flows through a Cisco IOS device. GET VPN combines the keying protocol Group Domain of Interpretation (GDOI) with IPsec encryption

to provide users with an efficient method of securing IP multicast traffic or unicast traffic. GET VPN enables the router to apply encryption to nontunneled (that is, “native”) IP multicast and unicast packets and eliminates the requirement to configure tunnels to protect multicast and unicast traffic.

By removing the need for point-to-point tunnels, meshed networks can scale higher while maintaining network-intelligence features that are critical to voice and video quality, such as QoS, routing, and multicast. GET VPN offers a new standards-based IP security (IPsec) security model that is based on the concept of “trusted” group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

For additional information about configuring GET VPN, see *https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-2mt/sec-get-vpn.html*

SGT over Ethernet Tagging

Cisco TrustSec (CTS) is an end-to-end network infrastructure that provides a scalable architecture for enforcement of role-based access control, identity-aware networking, and data confidentiality that helps to secure the network and its resources. CTS works by identifying and authenticating each network user and resource and assigning a 16-bit number called Security Group Tag (SGT). SGT is then propagated between network hops to allow intermediary devices (switches and routers) to enforce policies based on the identity tag.

CTS-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L2) layer. This feature is called L2-SGT imposition. This allows Ethernet interfaces on the device to be enabled for L2-SGT imposition to enable the device to insert an SGT in the packet that is to be carried to its next- hop Ethernet neighbor. SGT over Ethernet Tagging is a type of hop-by-hop propagation of SGTs embedded in clear-text (unencrypted) Ethernet packets.

For additional information about Cisco TrustSec, see https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/config.html

Crypto Engine Throughput Policing

There are two types of crypto throughput policing: Packet Rate Policing and Bit Rate Policing.

Packet Rate Policing

Cisco 921J router supports packet rate (packets/second) policing. The actual bit rate throughput (bits/second) depends on the packet sizes.

SKU	Packet Rate Limit (pps)
C921J	85616

Bit Rate Policing

Cisco 931 and C921 routers support bit rate (bits/second) policing.

SKU	Bit Rate Limit (Mbps)
C931	250
C921	150

Use the **show crypto engine accelerator statistic** command to see the packet drops due to policing. This example shows the output of the command for Cisco 921J router:

```
router#show crypto engine accelerator statistic

Device:   Onboard VPN
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 1440809 seconds ago
            95487781408 packets in               95486424592 packets out
         33644619163784 bytes in              33644414868202 bytes out
                  66273 paks/sec in                     66272 paks/sec out
                 186809 Kbits/sec in                  186808 Kbits/sec out
              497655085 packets decrypted           499488995 packets encrypted
         18274163849048 bytes before decrypt   15370455314736 bytes encrypted
         15369938845298 bytes decrypted        18274476022904 bytes after encrypt
                Last 5 minutes:
               26066232 packets in                   26066232 packets out
                  86887 paks/sec in                     86887 paks/sec out
              250994648 bits/sec in                 250995151 bits/sec out
             4247760866 bytes decrypted            4248382774 bytes encrypted
              114804347 Kbits/sec decrypted         114821156 Kbits/sec encrypted

Onboard VPN:
        ds: 0x10E31D10        idb:0x0EA74988

        Statistics for Virtual Private Network (VPN) Module:

        RAW API handler invoked:       997144123
        Available IPSEC static pak:          957
        Packets returned from drops:     1356816
        Pkts returned from raw rtrn:   997144110
        Available Pre-batch entries:         959

        Particle copy:                       0
        Particle swap:                       0
        Particle reparent:           998500926
        Packet overruns:                     0
        Output packets dropped:              0

        1440809 seconds since last clear of counters

CE Status Related Packet Stats
==============================
           Crypto Internal Error : 1
                 Resource Errors : 1356815

SKU information:
================
Max Bandwidth:250 Mbps  IMIX-size:365 Packets-per-second (PPS):85616
Statistics information:
  Packets handled 95486424673
  Packets dropped 1356815
```

This example shows the output of the command for Cisco 931 router:

```
Router#show crypto engine accelerator statistic
Device:   Onboard VPN
Location: Onboard: 0
               :Statistics for encryption device since the last clear
                of counters 2569 seconds ago
                    151982466 packets in                142427991 packets out
                  54548953852 bytes in                 51715073454 bytes out
                        59160 paks/sec in                    55441 paks/sec out
                       169858 Kbits/sec in                  161033 Kbits/sec out
                     67912187 packets decrypted            74515857 packets encrypted
                   27818735160 bytes before decrypt      26730230184 bytes encrypted
                   22213021398 bytes decrypted           29502075720 bytes after encrypt
                               Last 5 minutes:
                     22436614 packets in                  22436387 packets out
                        74788 paks/sec in                    74787 paks/sec out
                    219207775 bits/sec in                219204787 bits/sec out
                    3667993316 bytes decrypted           3670433984 bytes encrypted
                      99134954 Kbits/sec decrypted         99200918 Kbits/sec encrypted

Onboard VPN:
               ds: 0x12EA45B8        idb:0x123EF0D0

               Statistics for Virtual Private Network (VPN) Module:

               RAW API handler invoked:       142428045
               Available IPSEC static pak:          957
               Packets returned from drops:     9554448
               Pkts returned from raw rtrn:   142428044
               Available Pre-batch entries:         959

               Particle copy:                       0
               Particle swap:                70265739
               Particle reparent:            81716753
               Packet overruns:                     0
               Output packets dropped:              0

               2569 seconds since last clear of counters

CE Status Related Packet Stats
================================
          Crypto Internal Error : 1
                Resource Errors : 9554447

SKU information:
=================
Max Bandwidth:250 Mbps
Statistics information:
  Packets handled 142428045
  Packets dropped 9554447
```

This example shows the output of the command for Cisco 921 router:

```
Router#show crypto engine accelerator statistic
Device:   Onboard VPN
Location: Onboard: 0
               :Statistics for encryption device since the last clear
                of counters 3014 seconds ago
                     36412147 packets in                 33336964 packets out
                   13812996658 bytes in                 11412671776 bytes out
                         12081 paks/sec in                    11060 paks/sec out
```

```
                          36661 Kbits/sec in                   30290 Kbits/sec out
                       26024533 packets decrypted            7312452 packets encrypted
                    10920338080 bytes before decrypt      2892660426 bytes encrypted
                     8516694798 bytes decrypted           2895986384 bytes after encrypt
                                 Last 5 minutes:
                       14963577 packets in                  12694499 packets out
                          49878 paks/sec in                    42314 paks/sec out
                      146860315 bits/sec in                123543958 bits/sec out
                     2179066680 bytes decrypted           2349328596 bytes encrypted
                       58893694 Kbits/sec decrypted         63495367 Kbits/sec encrypted

Onboard VPN:
                ds: 0x135C41CC        idb:0x132B2FE0

                Statistics for Virtual Private Network (VPN) Module:

                RAW API handler invoked:        33336985
                Available IPSEC static pak:          957
                Packets returned from drops:     3075165
                Pkts returned from raw rtrn:    33336985
                Available Pre-batch entries:         959

                Particle copy:                       0
                Particle swap:              36412150
                Particle reparent:                   0
                Packet overruns:                     0
                Output packets dropped:              0

                3014 seconds since last clear of counters

CE Status Related Packet Stats
================================
                 Resource Errors : 3075165

SKU information:
=================
Max Bandwidth:150 Mbps
Statistics information:
  Packets handled 33336985
  Packets dropped 3075165
```