In-depth Overview of Network Security Features for Cisco Integrated Services Routers Generation 2

This white paper provides an in-depth overview of the network security features available on Cisco® 1900, 2900, and 3900 Series Integrated Services Routers.

Next-Generation Branch Security

Cisco 1900, 2900, and 3900 Series Integrated Services Routers are integral components of the Cisco solution and product portfolio, and deliver embedded security and VPN functions that allow organizations to identify, prevent, and adapt to network security threats in remote branches, right at the WAN perimeter.

The core security elements that enable routers to become critical devices for securing the network include:

- **Secure connectivity:** These features provide highly secure and scalable network connectivity, incorporating multiple types of traffic. Examples include IP Security (IPsec) VPN, Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), Enhanced Easy VPN, and Secure Sockets Layer (SSL) VPN.
- **Integrated threat control:** These features prevent and respond to network attacks and threats using network services. Examples include Cisco IOS® Firewall, Cisco IOS Intrusion Prevention System (IPS), Content Filtering, NetFlow, and Flexible Packet Matching (FPM).
- **Trust and identity:** These features allow the network to intelligently protect endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI).
- **Cisco network foundation protection:** These features protect the network infrastructure from attacks and vulnerabilities, especially at the network level. Examples include AutoSecure, Control Plane Policing and Protection, Source-Based Remote-Triggered Black Hole (RTBH) filtering, and Unicast Reverse Path Forwarding (URPF).

Secure Connectivity

Typical IP networks run innumerable applications, both legitimate and surreptitious, that compete with voice, video, and real-time data applications that are sensitive to performance. For example, voice traffic is sensitive to latency—voice packets are typically smaller and if they are queued behind large noncritical data packets, you can immediately perceive the degradation as audible clicks. Video traffic consumes high bandwidth and is sensitive to jitter; it is often impractical to buffer video data during delays, so packets are usually dropped with a view to quickly returning to a steady stream; if this packet loss happens too often, the result is a choppy stream and unhappy viewers.

These enterprise voice and video applications require sophisticated quality of service (QoS) and IP Multicast mechanisms to preserve voice and video quality. The premise of site-to-site and remote-access VPNs is to transport this traffic mix over encrypted ubiquitous and inexpensive public Internet access, for both primary and backup connectivity. Extending voice and video application quality over VPNs brings additional requirements in the form of integration of IPsec with QoS or IP Multicast. Voice over IP [VoIP] and IPTV are already mainstream, and Cisco TelePresence™ systems continue to grow in adoption. As these real-time voice and video telephony applications proliferate, so too do the VPN and security performance, scale, and feature integration requirements at the branch-office site.

Cisco 1900, 2900, and 3900 Series Integrated Services Routers deliver scalable VPNs with voice, video, and real-time data integration:

- **QoS:** Low-Latency Queuing (LLQ) before cryptography is a critical requirement to help ensure voice quality over VPNs. The embedded processor provides LLQ as well as postencryption interface-level QoS.
- **IP Multicast:** Secure Multicast is a foundational technology that combines the keying protocol, Group Domain of Interpretation (GDOI) with IPsec encryption to provide users an efficient method to secure IP Multicast traffic. It enables the router to apply encryption to nontunneled (that is, “native”) IP Multicast packets, increasing efficiency by eliminating the requirement to configure separate tunnels. Encapsulating IP Multicast packets allows IP Multicast routing (for example, Protocol Independent Multicast (PIM)) to route the packets even though they are encrypted. Native IP Multicast encapsulation also avoids the excessive packet replication that normally occurs with unicast tunnels. Secure Multicast is well suited for applications such as encryption of IP packets sent over satellite links, encryption in audio conferencing, secure real-time content replication, and DMVPN, among others.

Standard IPsec VPN

VPNs have been a fast-growing form of network connectivity, and as the adoption of VPNs grows, so do the performance, scale, and feature requirements, particularly in the fast-paced environment of the enterprise branch office. Well-suited solutions to these demanding networks are often single devices that can handle both remote-access and site-to-site VPNs, while offering multiple security services. Cisco 1900, 2900, and 3900 Series Integrated Services Routers include embedded acceleration for IPsec Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption and VPN processes.

The primary features provided follow:

- Acceleration of DES, 3DES, and AES (128, 192, and 256) encryption algorithms
- Support for Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication
- Use of Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity

For more information about Cisco IOS Software Standard IPsec, visit: http://www.cisco.com/go/ipsec

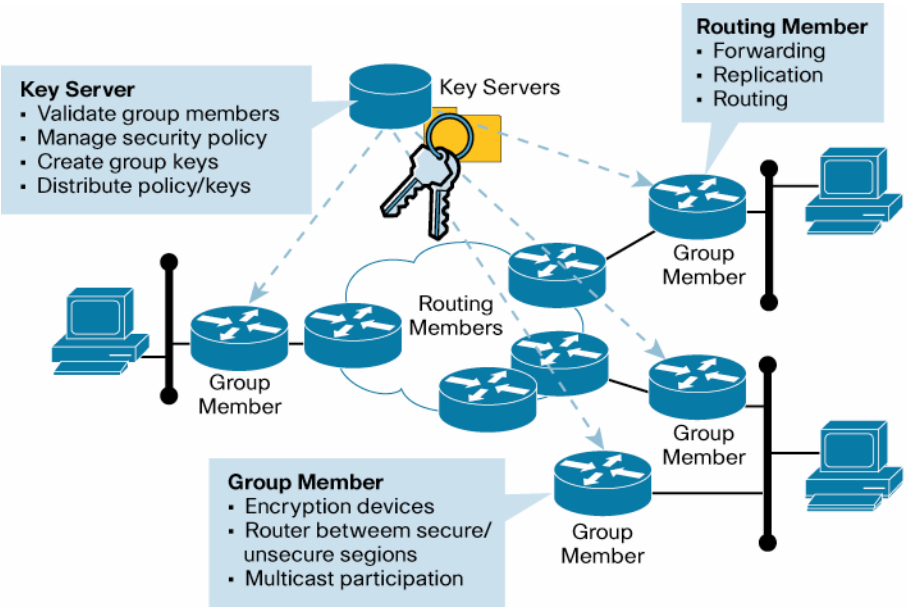
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html

Group Encrypted Transport VPN

With the introduction of Group Encrypted Transport VPN, Cisco now delivers an innovative, scalable category of VPN that eliminates the need for tunnels. It enables encrypted IP Unicast and Multicast packets to be routed directly to remote sites based on routing protocol decisions and to be rerouted around failed paths, providing enhanced availability. It enables organizations to rely on the existing Layer 3 routing information, thus providing the ability to address multicast replication inefficiencies and improving network performance. Distributed branch-office networks are able to scale higher while maintaining network-intelligence features critical to voice and video quality, such as QoS, routing, and multicast.

Group Encrypted Transport VPN offers a new standards-based IPsec security model that is based on the concept of "trusted" group members. Trusted group member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. A key server distributes keys and policies to all registered and authenticated group member routers (Figure 1).

Figure 1. Group Security Functions



Group Encrypted Transport VPN provides benefits to a variety of applications. Specifically, Group Encrypted Transport VPN:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- Maintains the network intelligence such as full-mesh connectivity, natural routing path, and QoS within Multiprotocol Label Switching (MPLS) networks
- Grants easy membership control with a centralized key server
- Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
- Reduces traffic loads on customer premises equipment (CPE) and provider-edge encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site

For more information about Cisco GET VPN, visit:

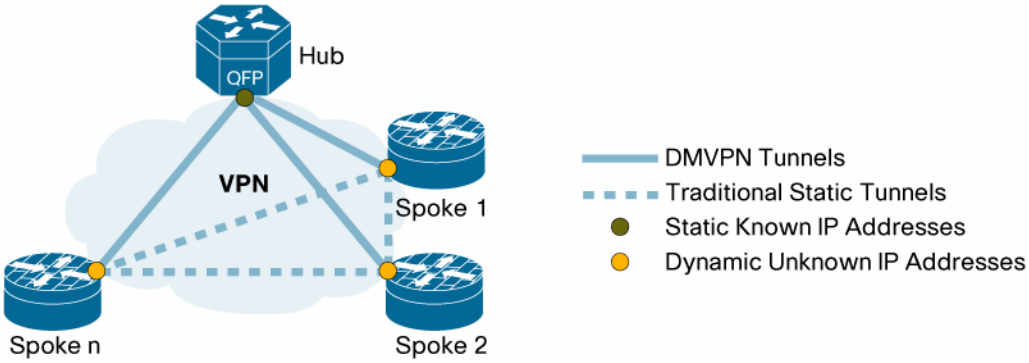
http://www.cisco.com/go/getvpn

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

Dynamic Multipoint VPN

Cisco routers offer DMVPN functions. Cisco DMVPN helps enable on-demand and scalable full-mesh VPN to reduce latency, conserve bandwidth, and simplify VPN deployments (Figure 2). The DMVPN feature builds upon Cisco IPsec and routing expertise by helping enable dynamic configuration of generic-routing-encapsulation (GRE) tunnels, IPsec encryption, Next Hop Resolution Protocol (NHRP), Open Shortest Path First Protocol (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP).

Figure 2. DMVPN



The power of DMVPN is truly reflected in the enterprise headquarters, where dynamic configuration of VPN tunnels combined with technologies such as QoS and IP Multicast optimizes the performance of latency-sensitive applications while simultaneously reducing administrative burden. For example, DMVPN allows you to obtain the same performance for voice and video applications over an IP transport network as you would over an alternate WAN link—securely and effectively.

DMVPN has been widely used to combine enterprise branch office, teleworker, and extranet connectivity. Major benefits include:

- Provision of full mesh connectivity with simple configuration of hub and spoke
- Automatic IPsec triggering for building an IPsec tunnel
- Facilitation of zero-touch configuration for addition of new spokes
- Support for dynamically addressed spokes

For more information about Cisco DMVPN, visit:

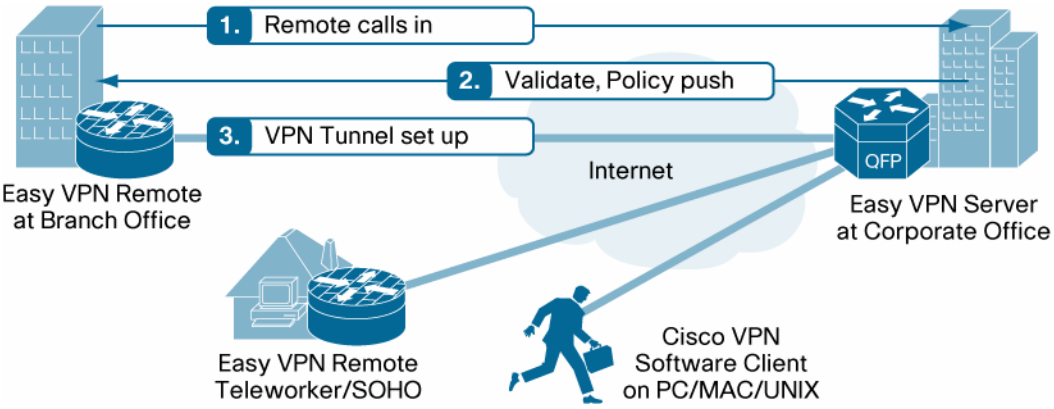
http://www.cisco.com/go/dmvpn

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_DMVPN.html

Easy VPN and Enhanced Easy VPN

For simple, high-scale, remote-access requirements, Cisco offers the Easy VPN solution, which uses a “policy-push” technology to simplify configuration while retaining rich features and policy control. Easy VPN Server, defined at the headquarters, pushes security policies to the remote VPN devices, helping ensure that those connections have up-to-date policies in place before the connection is established (Figure 3).

Figure 3. Easy VPN Tunnel Setup [[edits: setup (one word);;



Easy VPN offers the following benefits:

- Easy VPN supports both hardware (access routers) CPE and software remote-access clients using the same central-site router. You can install the Cisco VPN Client software on PCs, Macs, and UNIX systems to add remote-access connectivity to the router-based VPN at no additional cost. Because a single technology (Easy VPN) is used for both the hardware CPE and software clients, total cost of ownership (TCO) is reduced through simplification and unification of provisioning, monitoring, and AAA services.
- Easy VPN allows local (router-based), as well as centralized RADIUS and AAA authentication of both CPE routers and individual users.
- Easy VPN supports digital certificates, improving security over preshared keys.
- The technology enables load balancing of multiple central-site Easy VPN concentrators. Policy push of backup concentrator information to the CPE allows you to scale the solution without CPE reconfiguration.
- The technology provides virtualization of Easy VPN Server, allowing service providers to offer VPN services to multiple customers using a single platform.
- Easy VPN offers full-feature integration, including dynamic QoS policy assignment, firewall and IPS, split tunneling, and Cisco IP Service-Level Agreement (SLA) and NetFlow for performance monitoring.
- Cisco Configuration Professional provides wizard-based quick deployment of Easy VPN integrated with AAA and firewall, and real-time graphical monitoring of remote Easy VPN clients.
- Easy VPN is supported on all Cisco VPN product lines: Cisco IOS Software and Cisco Adaptive Security Algorithm (ASA) appliances.

When you integrate Enhanced Easy VPN features with Virtual Tunnel Interfaces (VTIs), you can configure virtual interfaces directly with Easy VPN, resulting in ease of deployment and advanced network integration. Benefits include:

- Configuration requirements at the headend, as well as at the remote branch offices, are greatly simplified.
- You can configure IP services using VTIs (or download the services from AAA servers), and at connection time, VTI instances are cloned dynamically from these templates. There is no need to manually create myriads of similar looking sets of configuration commands for each remote site.
- Offering per-user attributes such as QoS, VTI allows painless configuration of policies on a per-user basis, enabling administrators to be proactive in delivering the desired application performance and keeping users productive and motivated.
- VTI allows for configuration of each branch-office VPN tunnel with its own set of parameters, providing flexibility to customize configuration and security based on site-specific needs.

For more information about Cisco Easy VPN, visit:

http://www.cisco.com/go/easyvpn

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_rem.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_srvr.html

Cisco IOS SSL VPN

Cisco IOS SSL VPN is a router-based solution offering SSL VPN remote-access connectivity integrated with security and industry-leading routing features on a converged data, voice, and wireless platform. Using SSL VPN, companies can securely and transparently extend their business networks to any Internet-enabled location. Cisco IOS SSL VPN supports clientless access to applications such as HTML-based intranet content, email, network file shares, Citrix, and the Cisco SSL VPN client, enabling full network access remotely to virtually any application. Cisco Secure Desktop, as part of Cisco IOS SSL VPN, offers data-theft prevention even on noncorporate devices. Cisco Configuration Professional eases Cisco IOS SSL VPN deployment and performs real-time monitoring and management of SSL VPN sessions.

For more information about Cisco IOS SSL VPN, visit:

http://www.cisco.com/go/iossslvpn

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.html

Virtual Tunnel Interfaces

VPNs are increasingly being recognized as a mainstream solution for secure WAN connectivity. They replace or augment existing private networks that use leased lines, Frame Relay, or ATM to connect remote and branch offices and central sites more cost-effectively and with increased flexibility. This new status requires that VPN devices deliver higher performance, support for both LAN and WAN interfaces, and high network availability.

You can use the new Cisco IPsec VTI tool to configure IPsec-based VPNs between site-to-site devices. It provides a routable interface for terminating IPsec tunnels, thereby simplifying configuration. Cisco IPsec VTI tunnels provide a designated pathway across the shared WAN and encapsulate traffic with new packet headers, helping ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. In addition, IPsec provides true confidentiality (as does encryption), and can carry encrypted traffic.

With Cisco IPsec VTI, your enterprise can make full use of cost-effective VPNs and continue to add voice and video to your data network without compromising quality and reliability. The technology provides highly secure connectivity for site-to-site VPNs, enabling converged voice, video, and data over IP networks.

For more information about Cisco IPsec VTI, visit:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_virt_tunnl.html

Multi-Virtual Route Forwarding (VRF) Customer Edge and MPLS Secure Contexts

Multi-VRF CE, also referred to as VRF-Lite, provides the ability to configure and maintain more than one instance of a routing and forwarding table within the same physical router. In combination with Ethernet VLAN technologies and WAN VPN technologies such as Frame Relay, the technology helps enable provisioning of several logical services using one physical network, thereby extending privacy and security to the customer edge.

One Cisco router with Multi-VRF CE can support multiple companies with overlapping IP addresses, while maintaining a separation of data, routing, and physical interfaces.

For more information about Multi-VRF CE, visit:

http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html.

IPsec High Availability

Cisco VPNs support numerous features for deploying redundancy and load balancing. For smaller-scale headend IPsec deployments, you can use Hot Standby Router Protocol (HSRP) and Reverse Route Injection (RRI) to provide redundancy, whereas for larger deployments you can use Cisco Server Load Balancing (SLB) to provide redundancy as well as load balancing:

- **IPsec Stateful Failover:** IPsec Stateful Failover allows you to employ a backup IPsec server to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. The backup (secondary) IPsec server automatically takes over the tasks of the active (primary) router, without losing secure connections with its peers if the active router loses connectivity for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer. IPsec Stateful Failover is designed to work in conjunction with stateful switchover (SSO) and HSRP. HSRP provides network redundancy for IP networks, helping ensure that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. IPsec Stateful Failover provides protection for IPsec tunnels, IPsec with GRE, and Cisco IOS Easy VPN traffic.
- **HSRP and RRI:** RRI works with both dynamic and static cryptography maps to simplify network designs for VPNs requiring either high availability or load balancing. Routes are created for each remote network or host on the headend device to allow for dynamic route propagation. HSRP and IPsec dynamically reroute traffic to provide maximum availability of services. For hosts that do not have the ability to switch to another router if a primary router failure occurs, HSRP provides continuous network access. In this case, the HSRP virtual IP address is used as the VPN tunnel endpoint to provide continuous availability for stateless failover of IPsec.
- **SLB:** You can define virtual servers to represent a group of physical servers in a cluster of network servers (a server farm). When a client initiates a connection to the virtual server, Cisco IOS Software chooses a physical server for the connection based on a configured load-balancing algorithm. In case of a failure of a physical server, SLB dynamically reroutes all the incoming new IPsec sessions to the other server, thus providing redundancy.

For more information about IPsec High Availability, visit:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_vpn_ha_enhance.html.

Integrated Threat Control

Cisco Integrated Threat Control offers comprehensive network protection through simplified policy control and proactive system protection. This category of security functions includes features such as Cisco IOS Firewall, Cisco IOS IPS, Cisco IOS Content Filtering, NetFlow, Network-Based Application Recognition (NBAR), and Flexible Packet Matching (FPM). These features combine to:

- Protect network, servers, endpoints, and information
- Regulate network access, isolate infected systems, prevent intrusions, and protect critical business assets
- Counteract malicious traffic such as worms, viruses, and malware before they affect your business

Cisco IOS Firewall

Cisco IOS Firewall is a stateful firewall built into Cisco IOS Software that makes the Cisco 1900, 2900, and 3900 Series Integrated Services Routers an ideal security and routing solution in one device for protecting the WAN entry point into the network.

The primary features of Cisco IOS Firewall include:

- **Zone-based policies:** This feature allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones facilitates the application of firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface. Packets are not forwarded unless explicit zone-pair policies are specified in each direction, between each zone pair. The policy is written using Cisco Policy Language (that is, Modular QoS CLI [MQC]) and establishes the type of stateful inspection and session parameters that apply to each zone pairing. For example, the Internet-to-demilitarized zone (DMZ) boundary would require an explicit policy allowing HTTP and Domain Name System (DNS) to traverse.
- **Advanced Application Inspection and Control (AIC):** This feature uses inspection engines to enforce protocol conformance and prevent malicious or unauthorized behavior such as port 80 tunneling or misuse of email connectivity (Simple Mail Transfer Protocol [SMTP], Extended SMTP [ESMTP], point of presence 3 [POP3], and Internet Mail Access Protocol [IMAP]).
- **Firewall for secure unified communications:** Cisco IOS Firewall transparently supports voice traffic, including application-level conformance of media protocol call flow and the associated open channels. It supports voice protocols such as H.323v2, v3, and v4; Skinny Client Control Protocol (SCCP); and Session Initiation Protocol (SIP) and assures protection of unified communications components such as Cisco Unified Communications Manager, Cisco Unified Border Element, and their endpoints.
- **VRF-aware firewall:** Firewall is included in the list of services available at the individual context level for VRF deployments.
- **Firewall high availability:** Stateful firewall failover facilitates HSRP-based active-standby failover between two devices, avoiding disruption of active sessions.
- **Transparent firewall:** This feature provides Layer 2 segmentation, allowing easy addition of firewall into existing networks without renumbering IP subnets.
- **IPv6 firewall:** IPv6 firewall allows Cisco IOS Firewall to operate in mixed IPv6 and IPv4 environments.
- **Granular security policies:** This feature supports per-user, per-interface, or per-subinterface security policies.
- **Integrated identity services:** Integrated identity services provide per-user authentication and authorization.
- **Policy-based firewall management:** Cisco Security Manager and Cisco Configuration Professional provide intuitive policy-based ways to manage Cisco IOS Firewall.

For more information about Cisco IOS Firewall, visit:

http://www.cisco.com/go/iosfw

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html

Cisco IOS IPS

Some Cisco routers offer IPS functions. Cisco IOS IPS is an inline, deep-packet-inspection-based solution that helps Cisco IOS Software effectively mitigate network attacks. Cisco IOS IPS uses stateful packet-scanning techniques and attack and vulnerability signatures also available on various Cisco standalone intrusion-prevention-system (IPS) appliances and modules.

Now, with this IPS solution integrated into the existing access router, it is possible to implement additional lines of defense at the network edge, with minimal expense.

The major features of Cisco IOS IPS include:

- **Inline function:** Going beyond detection, this feature enables the router to respond immediately to security threats and protect the network. Routers can drop traffic, send an alarm, locally shun, or reset the connection

as needed, to stop attacking traffic at the point of origination and remove it from the network as quickly as possible. You can configure these actions per signature.

- **Signature Event Action Processor (SEAP):** Unique, risk rating based signature event action processor allows more accurate and efficient IPS event monitoring by filtering or separating events with low/high Risk Rating; dramatically improves the ease of management of IPS policies.
- **Ready-made signature files:** This feature allows users who want maximum intrusion protection to select an easy-to-use signature file that contains “most-likely” worm and attack signatures. Traffic matching these high-confidence-rated worm and attack signatures is configured to be dropped. Cisco Configuration Professional provides an intuitive user interface to provision these signatures, including the ability to upload new signatures from Cisco.com without requiring a change in software image, and configures the router appropriately for these signatures.
- **Customizable signatures:** With this feature you can modify an existing signature or create a new signature to address newly discovered threats (you can enable each signature action individually).
- **Transparent IPS:** This feature provides Layer 3 IPS for Layer 2 connectivity, permitting easy addition of IPS to existing networks with no IP subnet renumbering required.
- **VRF-aware IPS:** IPS is included in the list of services available at the individual context level for VRF deployments.
- **Large signature database:** The number of signatures from which to choose is ever-increasing; currently Cisco IPS sensor platforms support more than 1200 of the signatures.
- **Consistent management:** You can load and enable selected IPS signatures in the same manner as Cisco Intrusion Detection System (IDS) sensor appliances.

For more information about Cisco IOS IPS, visit:

http://www.cisco.com/go/iosips

Cisco IOS Content Filtering

Cisco IOS Content Filtering can help your organization protect itself from known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance. It monitors and regulates all Internet activities by blocking or restricting access to certain websites; provides protection from malicious sites that are known to give out malware, adware, spyware, and phishing; and helps your organization better manage network resources with simple and easy deployment.

The major features of Cisco IOS Content Filtering include:

- **Subscription-based services:** Easy-to-renew 1-, 2-, or 3-year subscription-based service is associated to the router platform; no individual user licenses are required. Your subscription provides access to Trend Micro's database, with content filtering policies set on the router.
- **Security ratings:** Cisco IOS Content Filtering protects against a variety of web-based threats, including zero-day attacks. It assesses the security risk posed by a website based on analysis from Trend Micro's TrendLabs, and it helps combat phishing and guards against spyware that may send confidential information to hackers and cybercriminals. TrendLabs provides the security rating for a given URL based on a combination of past behavior and current exposure to malware, adware, phishing, spyware, and hacking.
- **Category-based URL classification:** Content-based classification of URLs helps restrict access to objectionable or productivity-affecting websites (sites focusing on gambling or weapons, for example). More than 70 categories are available, including reputation-based blocking (spyware and keylogging, for example).
- **Keyword blocking:** Cisco IOS Content Filtering allows blocking of websites based on selected keywords that occur in the URL.

- **Black and white list support:** Cisco IOS Content Filtering supports 100 black and 1000 white URLs. For example, you can add trusted websites to a white list.
- **Management provisioning:** Cisco IOS Content Filtering is easy to use and deploy. It is managed through Cisco Configuration Professional, a web-based router management tool.
- **Caching:** The caching feature stores URL categories and their policy decisions (permit or deny) locally on the router, ensuring quick response time to access the Internet. Administrators can configure the cache duration on the router.

For more information about Cisco IOS Content Filtering, visit:

http://www.cisco.com/go/ioscontentfiltering.

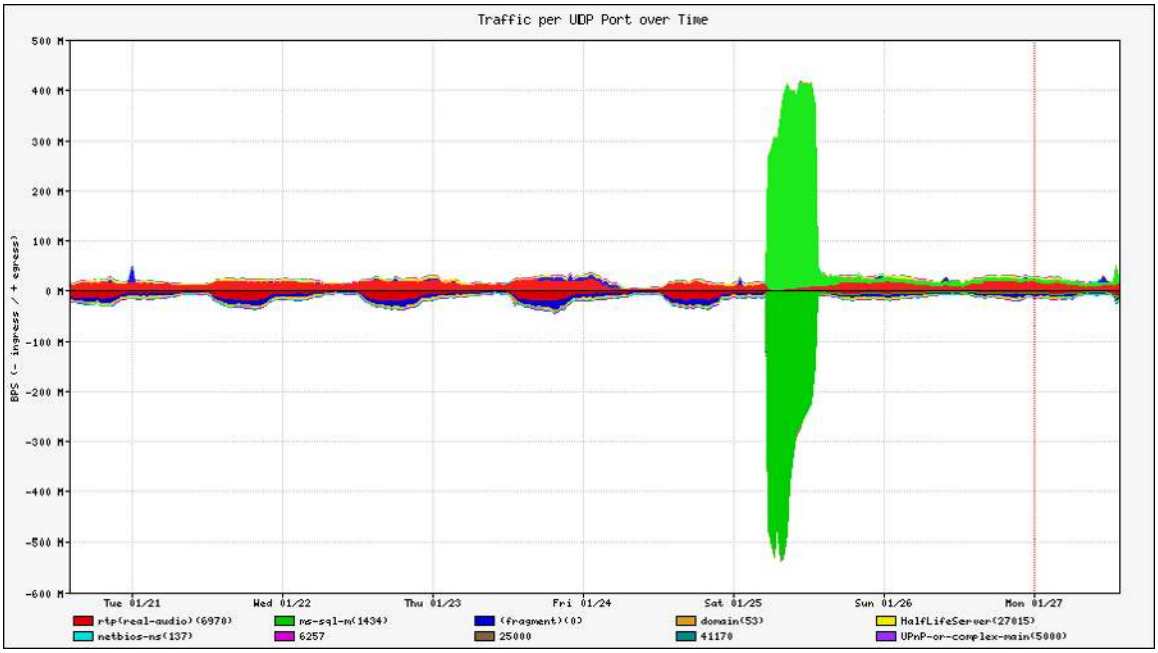
NetFlow

NetFlow is the primary technology in the industry to detect anomalies in networks. It supplies telemetry data to analyze IP traffic—for example, who is communicating to whom, over what protocols and ports, for how long, and at what speed.

Distributed denial of service (DDoS) attacks create sudden spikes in network use. These attacks can be quickly identified as abnormal network “events” when compared with typical traffic patterns gleaned from previously collected profiles and baselines.

By analyzing the detailed NetFlow flow data, one can also classify the attack (that is, the source and target of the attack), attack duration, and the size of packets used in the attack. Analysis tools include products from Cisco security partners as well as the Cisco Security Monitoring, Analysis and Response System (MARS). (Refer to Figure 4).

Figure 4. Example of Anomaly-Based DDoS Detection Using NetFlow and Arbor Networks



For more information about Cisco IOS NetFlow, visit: http://www.cisco.com/go/netflow.

For more information about Cisco Security MARS, visit: http://www.cisco.com/go/mars.

Network-Based Application Recognition

NBAR is a classification engine within Cisco IOS Software that uses deep and stateful packet inspection to recognize a wide variety of applications, including web-based and other difficult-to-classify protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments. When used in a security context, NBAR can detect worms based on payload signatures. When NBAR recognizes and classifies an application, a network can invoke services for that specific application. The technology also helps ensure that network bandwidth is used efficiently by working with QoS features to provide guaranteed bandwidth, bandwidth limits, traffic shaping, and packet coloring.

Cisco Configuration Professional includes an easy-to-use wizard to enable NBAR and also provides a graphical view of application traffic.

For more information about Cisco NBAR, visit: http://www.cisco.com/go/nbar.

Flexible Packet Matching

FPM inspects packets for characteristics of an attack and takes appropriate actions (log, drop, or Internet Control Message Protocol [ICMP] unreachable). It provides a flexible Layer 2 through Layer 7 stateless classification mechanism. You can specify classification criteria based on any protocol and any field of the traffic protocol stack. Based on the classification result, you can take actions such as drop or log on the classified traffic.

For more information about FPM, visit:

http://www.cisco.com/go/fpm

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_flex_pack_match.html

Trust and Identity

PKI Client (x.509 Digital Certificates)

Public Key Infrastructure (PKI) provides customers with a scalable and secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Cisco IOS Software supports embedded PKI client functions, which interoperate with the Cisco IOS certificate server and third-party certificate authorities.

The router generates a Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key), which establishes its legitimate identity. A Certificate Authority (CA) server validates the router and issues a digital certificate, granting admission into the PKI. Using the information in the certificate, each router in the PKI can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

The features supported by the PKI client include:

- **Certificate Servers:** Supports external (e.g. Verisign) or in-house (e.g. Microsoft) certificate servers; for smaller deployments Cisco IOS Software Certificate Server can be used
- **Certificate Authentication and Enrollment:** Supports SCEP, manual and TFTP methods
- **Auto Enrollment and Renewal:** Allows router to automatically request the digital certificate and renew prior to expiration; Certificate rollover allows seamless transition when CA's Certificate is renewed
- **Secure Device Provisioning:** Allows routers with factory-default configurations to be deployed securely using PKI and IPsec VPN, without extensive end-user configuration; ideal for remote offices or teleworker locations
- **PKI – AAA Integration:** Allows router to use an AAA server at the back-end to provide authorization; provides granular control based on certificate fields

- **Certificate Based Access Control:** Provides function similar to PKI – AAA Integration, except uses on-box ACLs to accept or reject certificates based on certificate fields
- **HTTPS management and SSL VPN features:** Supports persistent self-signed certificates
- **Certification Revocation Checking:** Supports Certification Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP)
- **Multiple-Tier CA Hierarchy:** Allows the router to work with CA TrustPoints at multiple levels; can be used to set up branch routers to work with departmental CAs or other subordinate certificate servers
- **PKI Credential (RSA Keys) Storage:** Allows the private key to be protected in NVRAM, with the option to encrypt the keys; also supports USB tokens
- **Other advanced PKI functions supported:** Erasure of RSA key when any user attempts to recover the password; multiple key pairs; import of key pair and certificates in PEM format; and 4096-bit public and private keys

For more information about Cisco IOS Software PKI Client, visit:

http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_pki_feat_rmap_ps6441_TSD_Products_Configuration_Guide_Chapter.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_white_paper0900aecd8046cbc4.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805249e3_ns855_Networking_Solutions_White_Paper.html

Cisco IOS Certificate Server

Cisco IOS Certificate Server embeds a certificate server into Cisco IOS Software, allowing the router to act as a certificate authority on the network.

Traditionally, it has been difficult to generate and manage cryptography information as VPN installations grow. The Cisco IOS Certificate Server addresses these challenges with a simple, scalable, easy-to-manage certification authority built onto the same hardware supporting IPsec VPN. Cisco IOS Certificate Server provides an important alternative to simple symmetric key deployments.

Features supported include:

- Simple Certificate Enrollment Protocol (SCEP)
- RSA key pair generation
- Database file storage
- Automatic archival of CA certificate and key
- Automatic CA certificate and key rollover when current certificate expires
- Certificate Revocation Lists (CRL)
- Subordinate and Registration Authority modes

For more information about Cisco IOS Software Certificate Server, visit:

http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_mng_cert_serv_external_docbase_0900e4b1805afd65_4container_external_docbase_0900e4b1807b4277.html

Standard 802.1x-Based Identity Services

Standard 802.1x applications make unauthorized access to protected information resources more difficult through the requirement of valid access credentials. By deploying 802.1x applications, network administrators can also effectively eliminate the possibility of users deploying unsecured wireless access points, addressing one of the greatest concerns of easy-to-deploy WLAN equipment.

For more information about 802.1, visit:

http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_ieee802_pba.html

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_ieee_loc_auth_sv.html

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_vpn_ac_802_1x.html

AAA

Cisco IOS Software AAA network security services provide the framework to set up access control on a router or access server. AAA is designed to allow administrators to dynamically configure the type of authentication and authorization they want on a per-line (per-user) or per-service (for example, IP, Internetwork Packet Exchange [IPX], or virtual private dialup network [VPDN]) basis, using method lists that are applied to specific services or interfaces.

For more information about Cisco IOS Software AAA, visit:

http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_4T/sec_securing_user_services_12.4t_book.html

Cisco IOS Network Foundation Protection

Continual availability of network infrastructure devices is even more critical at the enterprise headquarters. If a network router or switch is compromised, miscreants gain complete access to the entire network. Regardless of various skillful defenses that may be employed against attacks, it is necessary to protect against the unknown.

The following technologies emphasize the importance of robust network foundation protection, including self-defense for Cisco IOS Software devices if a DDoS attack occurs and secure management access to minimize the possibility of spoofing attacks on the management and control interface.

AutoSecure

Security configuration necessitates a detailed understanding of the security implications of each set parameter. An error or omission in configuring these parameters could jeopardize network security with an easily-exploited hole, compromising the availability, integrity, and privacy of the network information. Many network administrators have limited technical knowledge in terms of understanding the security implication of every Cisco IOS Software feature.

Cisco AutoSecure provides vital security requirements to enterprise and service provider networks by incorporating a straightforward, "one-touch" device lockdown process. It simplifies the security process by enabling the rapid implementation of security policies and procedures without requiring extensive knowledge of Cisco IOS Software features or the manual execution of the command-line interface (CLI). This feature offers a single CLI command that instantly configures the security posture of routers and disables nonessential system processes and services, thereby eliminating potential security threats.

You can deploy Cisco AutoSecure in one of its two modes, depending on the given customer deployment scenario:

- **Interactive mode:** Prompts you with options to enable and disable services and other security features
- **Noninteractive mode:** Automatically executes the AutoSecure command with the recommended Cisco default settings

For additional information about AutoSecure, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper09186a00801dbf61.html

http://www.cisco.com/en/US/products/ps6642/products_white_paper09186a0080183b83.shtml

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_autosecure.html

Control Plane Policing and Protection

Even the most robust software implementations and hardware architectures are vulnerable to DoS attacks. DoS attacks are malicious acts designed to cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the control plane processor. Distributed DoS (DDoS) attacks multiply the amount of worthless IP traffic, sometimes by as much as many gigabytes per second, by involving hundreds of sources. These IP streams contain packets that are destined for processing by the control plane of Cisco route processors. Based on the high rate of rogue packets presented to the route processor, the control plane is forced to spend an inordinate amount of time processing and discarding the DoS traffic.

To counter these and similar threats directed toward the heart of the system (that is, the processor), Control Plane Policing can employ a programmable policing function on routers that rate limits (or polices) traffic to the control plane. In conjunction with Cisco IOS QoS classification mechanisms, you can configure this policing function to identify and limit certain traffic types completely, or target only those that exceed a specified threshold level (Figure 5).

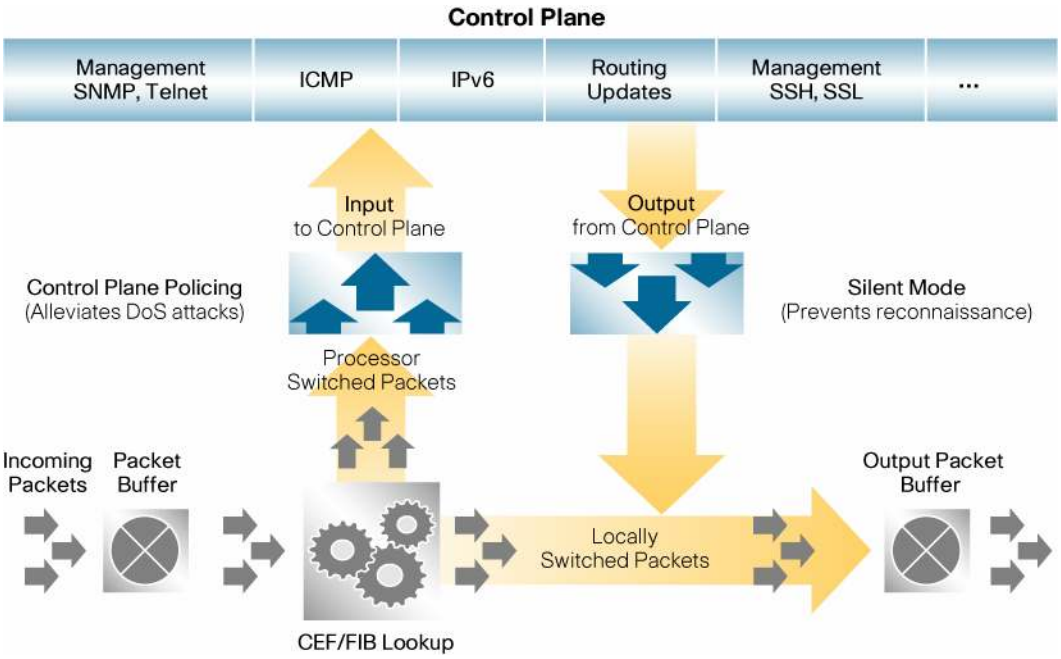
Control Plane Protection extends this policing functionality by allowing finer policing granularity.

For additional information about Control Plane Policing and Protection, visit:

http://www.cisco.com/en/US/products/ps6642/prod_white_papers_list.html.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlimt.htm.

Figure 5. Control Plane Policing: Packet Buffer; Incoming Packets; Cisco Express Forwarding and Forwarding Information Base (FIB) Lookup; Output Packet Buffer; and Silent Mode



CPU and Memory Thresholding Notification

CPU and memory are critical resources that mitigate the potential availability effect of the networking device. Simple Network Management Protocol (SNMP) MIBs currently enable a monitoring application to inquire as to the availability of a given resource. Because of the dynamic nature of these resources, scheduled polling of these variables often delays the action necessary to maximize network availability.

Memory Thresholding Notification enables you to manage the amount of memory consumed by various resource groups. You can specify the maximum amount of memory in bytes, or as a percentage of total processor resources. You receive notification when a resource group approaches its specified memory threshold.

With CPU Thresholding Notification, you can configure CPU usage thresholds, which trigger a notification when exceeded. Cisco IOS Software supports two CPU usage thresholds:

- **Rising threshold:** Percentage of CPU resources that trigger a CPU threshold notification when exceeded for a configured period of time
- **Falling threshold:** Percentage of CPU resources that trigger a CPU threshold notification when CPU usage falls below this level for a configured period of time

For more information about CPU and Memory Thresholding Notification, visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_cput.htm

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_memnt.html

Routing Protection

- MD5 neighbor authentication: MD5 neighbor authentication ensures that a router only receives reliable routing information and from trusted neighbors. Each routing update is hashed using the MD5 algorithm, and the resulting signature (digest) is sent as part of the routing update message. This provides the router with a way to certify the authenticity of each neighbor and the integrity of its routing updates.

- BGP TTL security check: TTL Security Check prevents routing-based DoS attacks, unauthorized peering and session reset attacks launched from systems not directly connected to the same subnet as the victim routers.
- TTL Security Check allows the configuration of a minimum acceptable TTL value for the packets exchanged between two eBGP peers. When enabled, both peering routers transmit all their traffic to each other with a TTL of 255. In addition, routers establish a peering session only if the other eBGP peer sends packets with a TTL equal to or greater than the TTL value configured for the peering session. All packets received with TTL values less than the predefined value are silently discarded.
- It is recommended that these features be enabled on all routers, but especially on those in contact with external peers. For more information on these features, please visit:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap3.html

ACL Protection

- ACLs protect edge routers from malicious traffic. They explicitly permit the legitimate traffic – for example routing and management traffic originating from authorized devices – that can be sent to the edge router destination address.
- IP Options Selective Drop: On most Cisco routers, a packet with IP Options is filtered and switched in software, due to the need to process the options and rewrite the IP header. This poses potential security threats, because malformed packets containing IP Options can adversely affect the performance of the device. ACL IP Options Selective Drop allows Cisco routers to filter packets that contain IP options or to mitigate the effects of IP options on a router by dropping these packets or ignoring the processing of the IP options.

For more information about ACL IP Options Selective Drop, visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/sel_drop.htm.

Secure Access Mode (Silent Mode)

One requirement for hacking a system is reconnaissance; that is, gaining information about the network. Hackers conduct reconnaissance by listening to system messages, such as the status of packet delivery, which provide information (IP addresses of devices, for example).

Secure Access Mode (also known as Silent Mode) is a new Cisco IOS Software feature designed to reduce the amount of information that a hacker can gather about a network. It stops the router from generating certain informational packets. For example, it suppresses the Internet Control Message Protocol (ICMP) messages and SNMP traps that are normally generated by the router. Like Control Plane Policing, Secure Access Mode takes advantage of the familiar MQC interface.

For more information about Secure Access Mode, visit:

https://www.cisco.com/en/US/products/ps6540/prod_bulletin09186a00801d7229.html#wp1002091

Raw IP Traffic Export

To perform a detailed security analysis of network traffic, many network administrators must attach a tool, such as protocol analyzers or mitigation servers. However, connection of these tools to the router currently requires inline insertion, which is operationally difficult.

The Raw IP Traffic Export feature is a lightweight Cisco IOS Software feature that exports IP packets as they arrive at or leave the networking device. A designated LAN interface exports captured IP packets out of the device. The objective is to export raw IP packets in their unaltered form to a designated device (such as a packet analyzer or IDS device).

Features of Raw IP Traffic Export include:

- Filter capability (using ACL) to help focus on exporting only interested traffic
- A sampling option that reduces the traffic output volume
- An option for you to specify an Ethernet port for exportation using either a MAC, 802.1q, or Inter-Switch Link (ISL) address associated with the destination host instead of an IP address
- The provision of syslog information when the feature is activated or deactivated

For more information about Raw IP Traffic Export, visit:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rawip.html.

Source-Based Remote-Triggered Black Hole Filtering

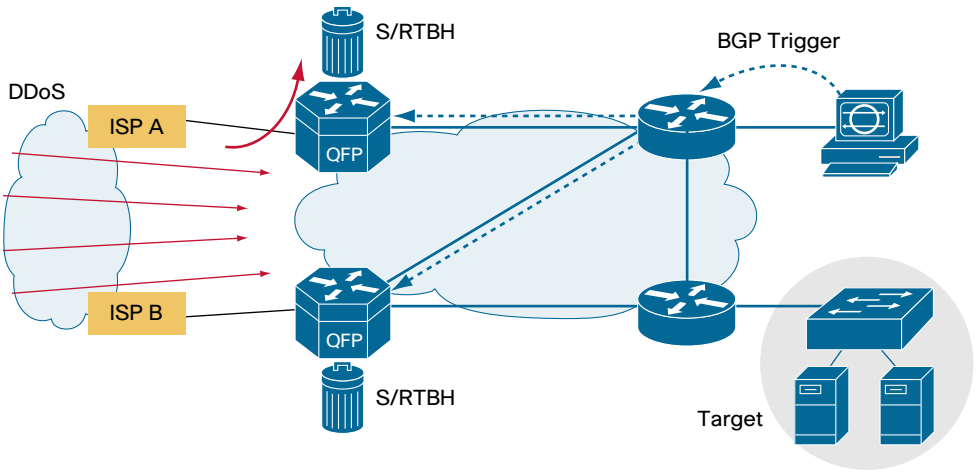
When your organization knows the origin of an attack (for example, by analyzing NetFlow data), you can apply containment mechanisms such as ACLs. When attack traffic is detected and classified, you can create and deploy appropriate ACLs to the necessary routers. Because this manual process can be time-consuming and complex, many customers use Border Gateway Protocol (BGP) to propagate drop information to all routers quickly and efficiently. This technique, termed Remotely Triggered Blackhole (RTBH), sets the next hop of the victim's IP address to the null interface. Traffic destined to the victim is dropped on ingress into the network.

Another option is to drop traffic from a particular source. This method is similar to the drop described previously but relies on the preexisting deployment of Unicast Reverse Path Forwarding (URPF), which drops a packet if its source is "invalid." Invalid includes routes to null0. Using the same mechanism of the destination-based drop, a BGP update is sent, and this update sets the next hop for a source to null0. Now all traffic entering an interface with URPF enabled drops traffic from that source. Although scalable, the BGP-triggered drops limit the level of granularity available when reacting to attack; they drop all traffic to the black-holed destination or source, as described previously. In many cases this reaction to a large attack is effective, and it certainly mitigates collateral damage (refer to Figure 6).

For more information about Source-Based RTBH Filtering, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd80313fac.pdf.

Figure 6. Real-Time Wire-Rate Defense Against DDoS Attacks with Source-Based RTBH Filtering



Unicast Reverse Path Forwarding

URPF helps limit the malicious traffic on an enterprise network. It works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. The Cisco 1900, 2900, and 3900 Series Integrated Services Routers support strict mode and loose mode.

When administrators use URPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. URPF configured in strict mode may drop legitimate traffic that is received on an interface that the router did not choose for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use URPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior with the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the null0 interface is dropped. You can specify an access list that permits or denies certain source addresses in URPF loose mode.

For more information about URPF, visit:
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_unicast_rpf.html

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_urpf_mib.html

Digital Image Signing

Digital Image Signing provides a way to establish the authenticity of the software image by appending a digital signature. A SHA-512 algorithm is used to compute a unique 64-byte hash for the software image. The hash is then encrypted using an RSA 2048-bit private key, and the resulting digital signature is appended to the software image.

During the software image loading process, the router uses its public key to decrypt the hash embedded in the image, and then verifies that the image is authentic. If the image has been altered by so much as a bit, the image is rejected, thereby protecting the device.

For more information about Digital Image Signing, visit:
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue.html.

Cisco IOS Software Login Enhancements

To control accessibility to the networking device, Cisco IOS Software requires that users log in to the device with a username and password. Unfortunately, hackers can exploit this requirement with dictionary attacks. In this attack, a hacker gains access to the device by programmatically trying all combinations of username and password.

Cisco IOS Software Login Enhancements offer a new time-based dimension to user login. Network administrators can use this feature to specify a time period between retries, alleviating dictionary attacks. User account lockout can now include a time period during which a user must succeed in order to log on to the device.

For more information about Cisco IOS Software Login Enhancements, visit:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html.

Role-Based CLI Access

Role-Based CLI Access allows the network administrator to define “views,” which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS Software. Views restrict user access to Cisco IOS Software CLI and configuration information and can define what commands are accepted and what configuration information is visible. Applications of Role-Based CLI Access include network administrators

providing security personnel access to specific functions. In addition, service providers can use this feature to grant limited access to end customers to aid in troubleshooting the network.

For more information about Role-Based CLI Access, visit:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli.html.

SSHv2

Secure Shell (SSH) Protocol Version 2 provides powerful new authentication and encryption capabilities. More options are now available for tunneling additional types of traffic over the encrypted connection, including file-copy and email protocols. Network security is enhanced by a greater breadth of authentication functions, including digital certificates and more two-factor authentication options.

For more information about SSH, visit:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_secure_shell_ps6441_TSD_Products_Configuration_Guide_Chapter.html

SNMPv3

SNMPv3 is an interoperable standards-based protocol for network management that provides secure access to devices by authenticating and encrypting packets over the network. The security features provided in SNMPv3 include:

- **Message integrity:** Helps ensure that a packet has not been tampered with in transit
- **Authentication:** Verifies that the message is from a valid source
- **Encryption:** Scrambles the contents of a packet to prevent it from being seen by an unauthorized source

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

For more information about SNMPv3, visit:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/snmpv3ae.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_snmp_supp.html

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

Summary

Cisco security routers offer multiple security technologies to protect remote offices, teleworkers and mobile users. These include site-to-site and remote access VPN technologies that provide privacy and data integrity; perimeter security, intrusion prevention and day zero protection capabilities; trust and identity protection capabilities, as well as foundational security features. Each of these could in itself justify the incremental capital costs of purchasing security on the router. In addition, the ease of deploying and managing Cisco security routers ensures that the total cost of ownership is low, allowing the solution to accumulate substantial value over time.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-556320-00 09/09