

Turn It On: Use Embedded Cisco IOS Cyber Security Features for Your Network

What You Will Learn

To get the most functionality, value, and return on investment (ROI) from your Cisco® infrastructure, you should be aware of its many features. This document describes the embedded features that enhance network security by increasing:

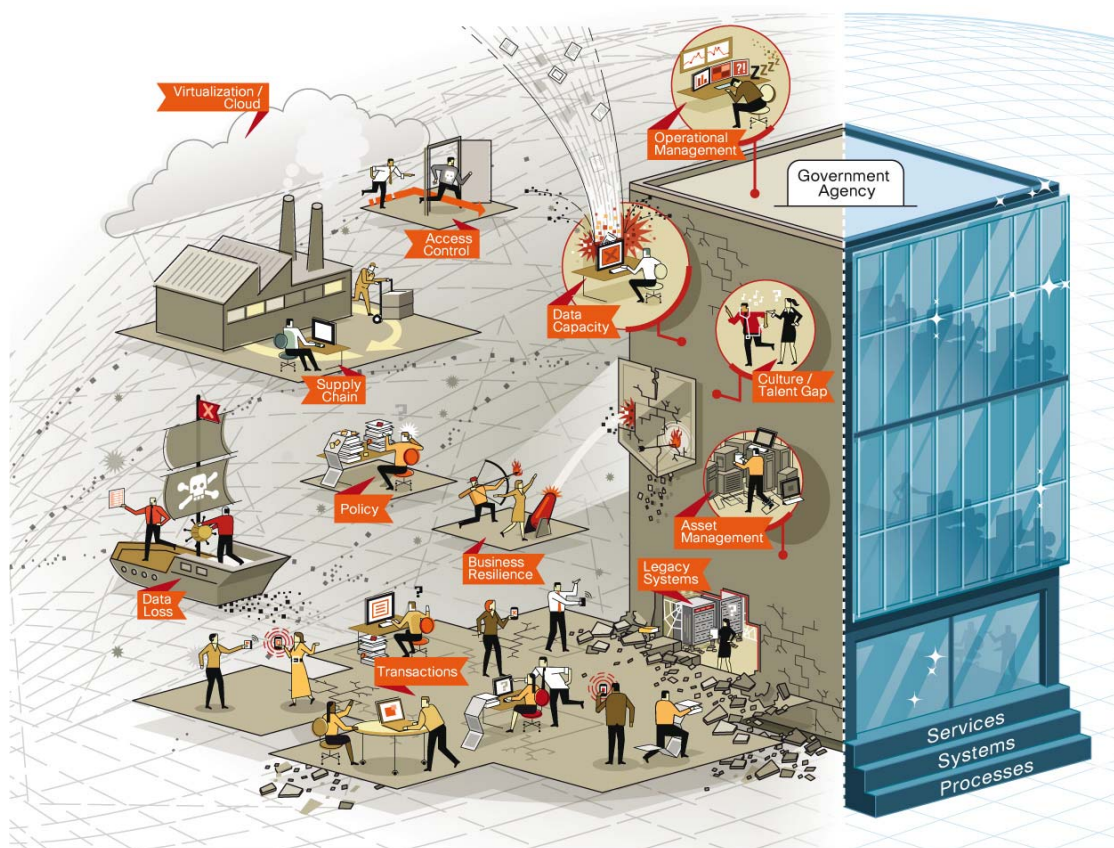
- Trust
- Visibility
- Resiliency.

The Cisco [Turn it On](#) program is designed to empower agencies like yours to take full advantage of Cisco's powerful core networking solutions.

Today's Challenges

Figure 1 illustrates some of the challenges facing today's networks.

Figure 1. The Secure Network



The global adoption of IP has changed the way citizens, businesses, and governments interact. Today, the most prevalent communications platform is the Internet. Over the past 10 years, worldwide Internet growth has increased

over 400 percent, with an estimated 29 percent of the world population, or almost 2 billion people, being Internet users. In the United States alone, an estimated 77 percent of the population, or roughly 240 million people, are broadband Internet service users.

Unfortunately, the benefits and efficiencies of the modern IP network apply equally to any undertaking regardless of intent - to a student researching a topic or a malicious hacker attempting to steal or cause disruption. Adding to the challenge is the move from network-centric to network-dependent control processes. IP-connected devices and form factors are increasing in number and becoming integrated into every modern industry. Our diplomatic, intelligence, military, and economic stability is ever more dependent on the IP network. On any given day new threats, vulnerabilities, and security breaches across industry and government are discussed in the media. Challenges such as information rights, virtualization, asset management, and outdated systems are just a few of the topics that the modern network-dependent organization needs to address.

Solution

Although IP networks serve as the conduit for today's threats, networks are also the first and natural location in which these threats can be mitigated. No single company can solve the complex challenges presented by the Internet, but the inherent role of the network positions Cisco as a natural partner in developing and executing a successful network security strategy. Cisco identifies three considerations within the complex environment surrounding Internet security: trust, visibility, and resilience. Each of these considerations requires people, process, and technology, and for each, you can use the network to manage risk and improve your organization's security posture:

- Trust: Identify and manage
- Visibility: Prevent and detect
- Resilience: Respond, recover, and report

Trust: Identify and Manage

Network security can be a complex topic, but there are many simple and basic functions that organizations must do and do well: managing IT assets to create layers of protection and checks and balances for network behavior. Knowing what is on your network and knowing that it is authorized, configured properly, and not exposed to undue risk are the most important first steps. Another critical step is making sure that your infrastructure is designed to the standards necessary to reduce risk and maintain resilience.

Visibility: Prevent and Detect

The Internet-connected world presents global threats that must be monitored and understood. Technologies like Cisco SensorBase provide quick detection and mitigation of known threats. The more complex threats require using the enterprise network to identify behaviors and patterns and to quickly remove suspicious behaviors. You can take advantage of the inherent sensing capability of the network and use accounting resources to create an organizational risk picture and situational awareness.

Resilience: Respond, Recover, and Report

It is clear that the basics matter and that while handling known threats is good, preparing for unknown threats is better. When those advanced threats materialize, maintaining your overall operations and network resilience is vital to managing the chaos of network disruption. As you manage through the chaos, mitigation is primary. The ability to remediate and understand how the successful attack could occur helps you to make sure a similar attack does not have the same chance of success.

Technical Overview

Cisco IOS® Software includes features that can give your organization better network security today. With better security, you can deal with threats in a more controlled manner, and develop a process for identifying, managing, and

defeating an Internet attack. The same features may have other uses such as improving Quality of Service (QoS), but when they are enabled they also provide critical information as well as protection for the network cybersecurity. Cisco wants you to get the most out of equipment already deployed by turning on these features to enhance your network protection today. Along with your expertise, these tools empower you to take full advantage of Cisco's powerful core networking solutions to maximize your productivity, efficiency, and technology investment.

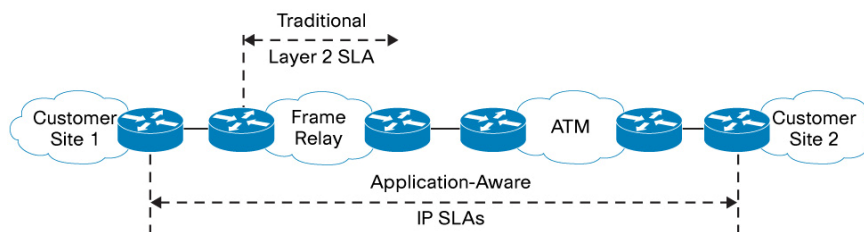
The rest of this document describes how to use features of your Cisco IOS network to improve your cybersecurity posture today, by addressing the security considerations.

- **Trust:** Identify and manage threats using technologies such as IP service-level agreements (IP SLAs) and Control Plane Policing (CoPP)
- **Visibility:** Prevent and detect incidents using Cisco NetFlow
- **Resilience:** Respond, recover, and report after an incident using technologies such as Network-Based Application Recognition (NBAR) and Peer-To-Peer (P2P) blocking (policy class mapping)

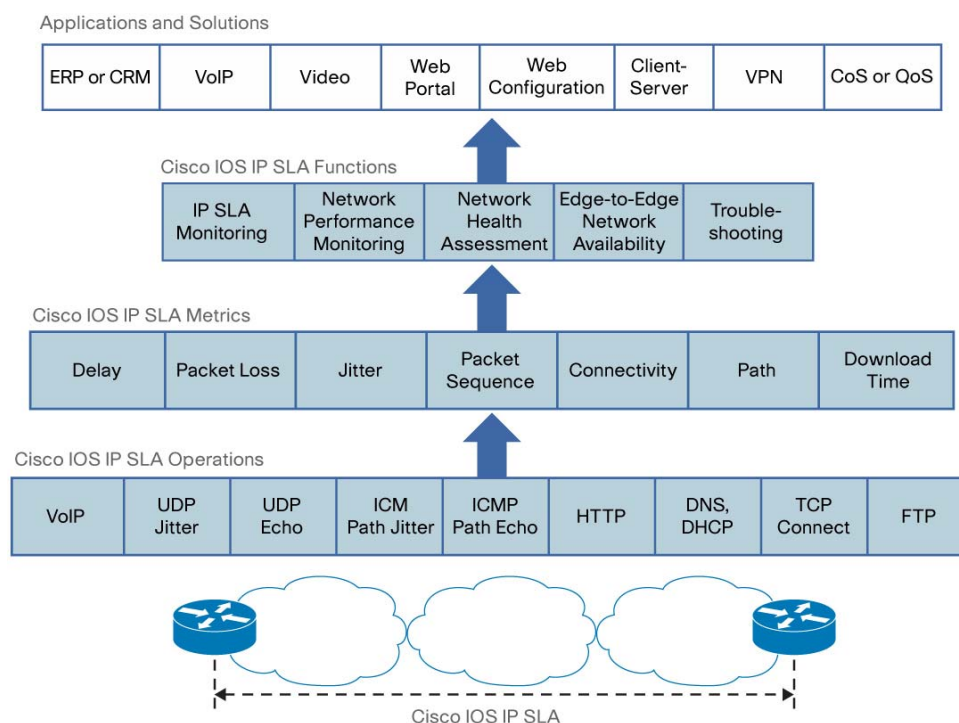
IP SLAs and Network Cybersecurity

An IP-SLA is the formalization of the agreed QoS in a contract between a customer and a service provider. For public-sector organizations, IP SLAs are service agreements between the agency, contractor, and end users. Cisco IOS IP SLAs help customers to assure mission-critical applications and services that use data, voice, and video in an IP network. Cisco has augmented traditional service-level monitoring and reinvented the IP infrastructure to become IP application-aware, by measuring end-to-end SLAs as well as the IP layer (Figure 2).

Figure 2. Comparison of Traditional SLAs and Cisco IOS IP SLAs



With Cisco IOS IP SLAs, users can verify service guarantees, increase network reliability by validating network performance, and proactively identify network cyber intrusions. These SLAs use active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus supporting the measurement of network performance and condition (Figure 3).

Figure 3. Cisco IOS IP SLA Technology

Cisco IOS IP SLA Capabilities

Cisco IOS IP SLAs measure the following parameters:

- Latency (delay): propagation delay, serialization delay, and queuing delay
- Jitter
- Packet loss
- Burst loss (multiple packets)
- Packet reordering

Through these measurements, your Cisco IOS router can be turned into an active probing device for Internet security.

Cisco IOS IP SLAs also provide the following benefits:

- Wide measurement capabilities: User Datagram Protocol (UDP), TCP, and Internet Control Message Protocol (ICMP)
- Near-millisecond precision
- Accessibility through the command-line interface (CLI) and Simple Network Management Protocol (SNMP)
- Proactive notification
- Historical data storage
- Flexible scheduling options
- Current availability in Cisco IOS Software (on most platforms)
- Support for almost all physical and logical interfaces

How IP SLAs Promote SCybersecurity

IP SLAs are a baseline feature of the Cisco IOS Software that is already in your router. By turning IP SLAs on, you can monitor traffic and resolve problems. Traffic monitoring is a critical cybersecurity feature because it provides information on who is accessing your network at what times. IP SLAs also allow your network to perform to set

standards. When you reach the upper limits of those settings, you know you have a problem. More importantly, you know whether the problem is one that can be resolved internally or represents an actual intrusion on the network.

Within the realm of network cybersecurity, Cisco IOS IP SLAs can be used as a verification toolset to provide proper deployment, posturing, configuration, and placement of network-related devices with respect to SLAs. One example would be to use IP SLAs to continually verify reachability and performance level of a mission-critical applications during a distributed-denial-of-service (DDoS) incident.

Validating QoS in Real Time

The use of Cisco IOS IP SLAs provides continuous validation of QoS policies throughout the network. This helps to ensure that agency networks are prepared to provide valid QoS for mission-critical applications, even in the midst of an intrusion.

You can also use IP SLAs in conjunction with the Cisco IOS Embedded Event Manager (EEM). For example, if you use an IP-SLA to monitor the availability and bandwidth of a mission-critical application, and if those metrics fall into an unsafe zone, EEM would instruct the local IOS network device, a router in this case, to redirect the traffic to a secondary path that has bandwidth available.

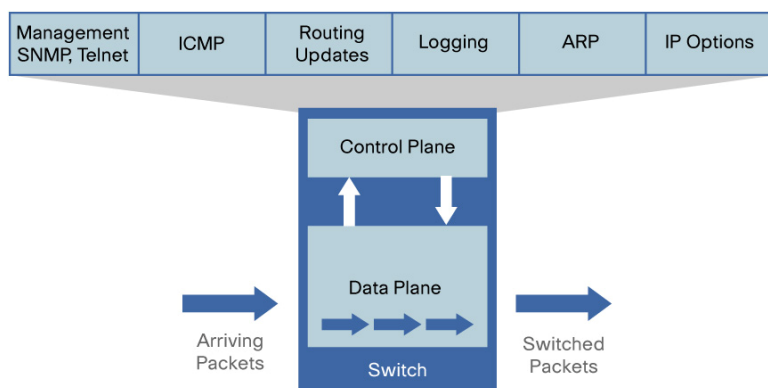
For more information about using Cisco IOS IP SLAs, visit:

- http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps10777/whitepaper_c11-584889_ps6815_Products_White_Paper.html
- <http://www.cisco.com/go/ipsla>

Cisco IOS CoPP and Network SCybersecurity

The Cisco IOS Control Plane Policing feature allows you to configure a QoS filter that manages the traffic flow of control plane packets (Figure 4) to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial of service (DoS) events. By turning on this feature, you can maintain packet forwarding and protocol states despite an intrusion or heavy traffic load on the router or switch.

Figure 4. Control Plane Processes

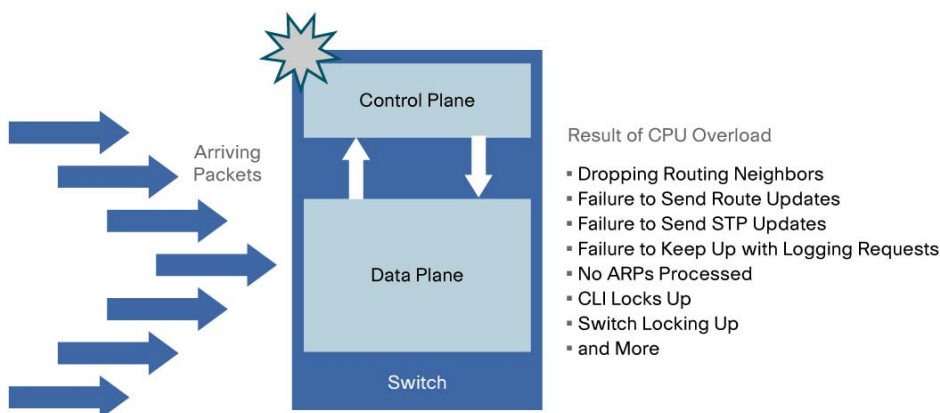


A DoS incident targeting a route processor module (RPM) can cause serious issues, including: high RPM CPU utilization (near 100 percent), loss of line protocol keepalives, and routing protocol updates, leading to route flaps and major network transitions. Interactive sessions through the CLI are slow or completely unresponsive due to high CPU utilization. Packet queues back up, leading to indiscriminate drops (or drops due to lack of buffer resources) of other incoming packets (Figure 5).

One vector an intruder uses to initiate a DDoS incident is to move against security devices, which in turn prevents the attacked agency from deploying countermeasures because of a lack of access to the network security devices for

enforcement. If you turn on CoPP, the Cisco IOS device provides you a dedicated conduit of access even during a DDoS or similar intrusion.

Figure 5. DDoS Overloads CPU, Which Drops Packets



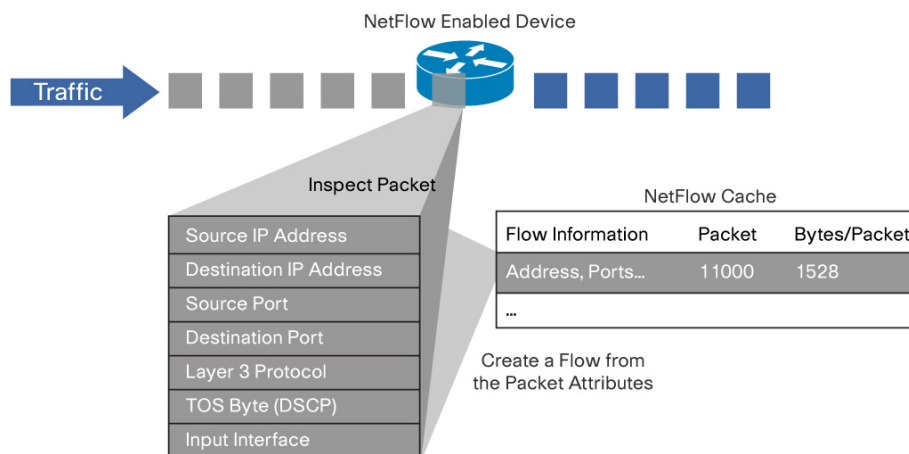
Cisco IOS NetFlow and Network Security

NetFlow is embedded within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. In response to new requirements and pressures, network operators are finding it critical to understand how the network behaves normally as a baseline to compare how it works when attacked, including:

- Application and network usage
- Network productivity and use of network resources
- Effects of changes to the network
- Network anomaly and security vulnerabilities
- Long-term compliance issues

Cisco IOS NetFlow fulfills these needs, creating an environment where administrators have the tools to understand who, what, when, where, and how network traffic is flowing (Figure 6). When network behavior is understood, processes improve and an audit trail of network use is available. This increased awareness reduces the vulnerability of the network to outage and allows efficient operation.

Figure 6. Creating a Flow in the NetFlow Cache



Cisco IOS NetFlow gives network managers a detailed view of application flows on the network. For more information about how Cisco IT uses NetFlow, visit

http://www.cisco.com/application/pdf/en/us/guest/products/ps6601/c1042/cdccont_0900aecd80311fc2.pdf.

Using IP Flows to Provide Network Information

Cisco IOS NetFlow examines each packet that is forwarded within a router or switch for a set of IP packet attributes. These attributes are the IP packet identity of the packet and determine whether the packet is unique or is similar to other packets. Traditionally, an IP flow is based on a set of five to seven IP packet attributes.

Figure 7. Example of a Cisco IOS NetFlow Cache

1. Flow Cache - The First Unique Packet Creates a Flow

SrcIfl	SrcIPadd	DstIfl	DstIPadd	Protocol	TOS	Figs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/Pkt	Active	Idle
Fa 1/0	173.100.21.2	Fa 0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa 1/0	173.100.3.2	Fa 0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa 1/0	173.100.20.2	Fa 0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa 1/0	173.100.6.2	Fa 0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Flow Aging Timers

- Inactive Flow (15 Sec Is Default)
- Long Flow (30 Min (1800 Sec) Is Default)
- Flow Ends by RST or FIN TCP Flag

SrcIfl	SrcIPadd	DstIfl	DstIPadd	Protocol	TOS	Figs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/Pkt	Active	Idle
Fa 1/0	173.100.21.2	Fa 0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Flows Packaged in Export Packet
Nonaggregated Flows: Export Version 5 or 9

4. Transport Flows to Reporting Server



IP packet attributes used by Cisco IOS NetFlow include:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- Class of Service (COS)
- Router or switch interface

All packets with the same source and destination IP address, source and destination ports, protocol interface, and COS are grouped into a flow, and then packets and bytes are tallied. This methodology of determining a flow is scalable because a large amount of network information is condensed into a database of NetFlow information called the NetFlow cache.

NetFlow Dynamic Top Talkers CLI

The Cisco IOS NetFlow Dynamic Top Talkers CLI feature gives you an overview of the highest volume traffic in your network by aggregating flows on a common field. Top talkers are other websites from which you receive the most traffic. For example, you can aggregate all of the flows for a destination network by aggregating them on the

destination IP address prefix. There are over 20 fields from flows on which you can aggregate the highest volume traffic.

For network security, identifying top talkers can help you determine who is attempting a DDoS and where that traffic is coming from. A DDoS is coordinated so that multiple machines that have been infected target your network at once. Seeing that all your top talkers are performing the same network behavior is invaluable, because you can stop that access without shutting down other parts of your network, or letting the intrusion crash your network.

NetFlow Data Access

There are two primary methods to access Cisco IOS NetFlow data: the CLI and an application reporting tool. If you need an immediate view of what is happening in your network, the CLI can be used. The NetFlow CLI is very useful for troubleshooting.

The other choice is to export NetFlow data to a reporting server called the NetFlow Collector (NFC). The NFC assembles and interprets the exported flows and combines or aggregates them to produce valuable reports used for traffic and security analysis. NetFlow export, unlike SNMP polling, pushes information periodically to the NetFlow Collector. In general, the NetFlow cache is constantly filling with flows, and software in the router or switch is searching the cache for flows that have terminated or expired; these flows are exported to the NFC. Flows are terminated when the network communication has ended (indicated when a packet contains the TCP FIN flag). The following steps are used to implement NetFlow data reporting.

- NetFlow is configured to capture flows to the NetFlow cache
- NetFlow export is configured to send flows to the NFC
- The NetFlow cache is searched for flows that have terminated, so the flows can be exported to the NFC
- Approximately 30 to 50 flows are bundled together and typically transported in UDP format to the NFC
- The NFC software creates real-time or historical reports from the data

NetFlow and Internet Security

Cisco IOS NetFlow improves your Internet security posture by providing the following.

- A distributed sensor in the network: NetFlow tracks data flows across the entire network, providing a distributed view of the network. From each device using NetFlow, the administrator can gather information on how that machine's data flows across the network. The administrator can pinpoint a disruption of service or spike in a data flow, which could be the source of a security breach.
- Anomaly, discovery, and correlation: If there is an anomaly in the network flows, NetFlow helps the administrator to discover it. If a series or group of anomalies is present, NetFlow provides the data that can be used to correlate the anomalies. Correlation is then used to identify which anomalies are intrusions on the network.
- Security Information and Event Management Systems (SIEMs): When combined with SIEMs and correlated with data from other devices and layers, NetFlow becomes indispensable. SIEMs use NetFlow data to correlate information to determine if there is a network attack and where it is coming from. NetFlow data is aggregated with data from other sources such as IPSs, firewalls, VPNs, the application layer, and in some systems, identity data. This data is then correlated using several types of techniques, including:
 - Rules-based
 - Statistical
 - Historical
 - Vulnerability

These correlations are conducted for each monitoring site and also across websites. This correlated data is prioritized based on traffic flows, intrusions within a site, or intrusions across sites. A risk analysis is then performed to discover which intrusion has the greatest potential for harm to the enterprise. Ideally this risk assessment will at least analyze the following:

- Agency processes
- Network processes
- Sites compared to enterprise

The most important security benefit of combining NetFlow with SIEMs is the improvement in security insight and response. With real-time NetFlow views, priority-based alerts can be created. Threats can also be correlated with other vectors, so that the highest-priority problems are seen first and administrators can respond accordingly.

- Incident usage of top talkers on the CLI: NetFlow also informs the administrator about which top talkers are currently using the network. For example, a report is generated identifying the top talkers. If the top talkers are using too much bandwidth, that bandwidth can be restricted or blocked as needed.

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

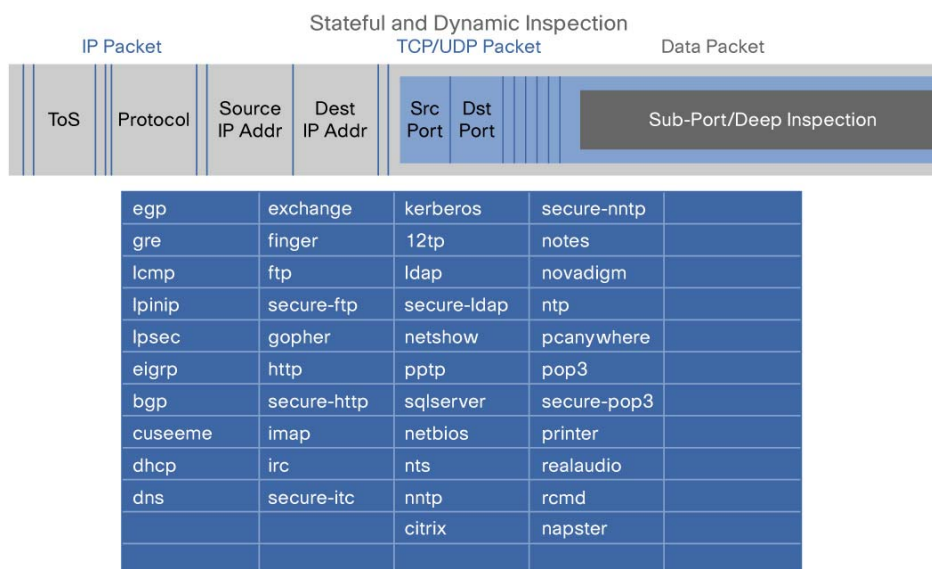
For detailed technical IOS documentation on NetFlow, visit http://www.cisco.com/en/US/products/ps6601/prod_white_papers_list.html.

Cisco IOS NBAR and Network SCybersecurity

Cisco IOS NBAR is a powerful classification engine that recognizes and classifies a wide variety of applications. NBAR works with QoS features to help ensure that network bandwidth is best used to fulfill agency objectives. Use NBAR to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately so both your network and the service provider’s network can provide end-to-end QoS.

NBAR helps ensure performance for mission-critical applications by intelligently classifying applications, providing absolute priority and a guaranteed amount of bandwidth. In addition, NBAR limits the bandwidth consumed by less critical applications. Figure 8 shows the applications supported by NBAR.

Figure 8. Applications Supported by NBAR



Packet Description Language Module (PDL)

NBAR and Network SCybersecurity

In a DoS or DDoS incident, someone is trying to overwhelm your network capacity, to prevent your mission-critical applications from functioning. Turning on NBAR mitigates such an event because critical applications have priority over the traffic generated by the intrusion. Critical applications continue to send traffic, while NBAR drops selective packets to avoid congestion. This limits the amount of traffic your network will dedicate to the intruder's request for data. By setting up NBAR you further mitigate the ability of a DoS or DDoS attack to be successful at the onset.

NBAR and Peer-to-Peer Traffic

A Cisco IOS router can use NBAR to block peer-to-peer (P2P) traffic from inside the network to the Internet.

NBAR recognizes specific network protocols and network applications that are used in your network. Once a protocol or application is recognized by NBAR, you can use the Cisco Modular QoS CLI (MQC) to group the packets associated with those protocols or applications into classes, on the basis of whether the packets conform to certain criteria.

For NBAR, the criterion is whether the packet matches a specific protocol or application known to NBAR. Using the MQC, network traffic with one network protocol (Citrix, for example) can be placed into one traffic class, while traffic that matches a different network protocol (gnutella, for example) can be placed into another. Later, the network traffic within each class can be given the appropriate QoS treatment by using a traffic policy (policy map).

For more information on classifying network traffic using NBAR, visit

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar_ps6441_TSD_Products_Configuration_Guide_Chapter.html.

The capacity of NBAR to block P2P traffic is important for network security because P2P traffic provides an opportunity for data to be leaked. The U.S. Federal Trade Commission (FTC) has notified nearly 100 public and private organizations in 2010 that they are leaking sensitive data through P2P file-sharing networks. The compromised data include health information, financial records, and license numbers of employees and customers. If companies do not take adequate measures to protect sensitive data from exposure, they could be found in violation of U.S. data protection laws, such as the Gramm-Leach-Bliley Act and Section 5 of the FTC Act.

Conclusion

Several features in Cisco IOS Software can help you deploy a more secure network. When you turn these features on, they make your network more resilient and provide better Internet security. These features provide insight into how traffic flows on your network and how an intrusion can occur.

Cisco is the leading provider of a comprehensive solution that addresses critical infrastructure security requirements outlined in the Comprehensive National Cybersecurity Initiative (CNCI). Fundamental areas of concern include classified networks, data access and retrieval, remote access, detection and prevention of external and internal attacks, protecting the evolving data centers, supporting the move to cloud-based computing, and securing the government supply chain.

The growth of the Internet population, network-connected devices, and dependence on modern networks make it urgent to counteract network threats. To continue prospering from the use of this technology, all organizations must address this challenge. Cisco is a natural partner in any enterprise security strategy, because the network platform plays an important role in this environment. To keep pace with today's dynamic environment, you must learn to use the network to achieve trust, gain visibility, and provide resiliency in your enterprise.

For More Information

A tremendous amount of information is available about Cisco security features, including videos, webinars, and white papers. This information is available from your Cisco service representative or from <http://www.cisco.com>.

For more information about the features emphasized in the Cisco Turn It On program, visit http://www.cisco.com/web/strategy/government/usfed_tio.html.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)