The Self-Defending Network for the Service Provider – Cisco's Contribution to Defense in Depth

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 4.0c

Option 1 - Research on Topics
in Information Security

Submitted by: Stuart Mark
Location: Calgary, AB – Canada
23rd March 2005

Paper Abstract: This paper provides an overview of the Cisco Self-Defending Network strategy and examines how it might fit into a service provider context.

Table of Contents

Abstract/Summary 1
Introduction 2
The Self-Defending Network 3
  The Integrated Services Router 3
  Trust and Identity 5
    Network Admission Control (NAC) 5
    Identity-Based Network Services - IEEE 802.1x 6
    Authentication, Authorization and Accounting (AAA) 7
  Network Infrastructure Protection 8
    Control Plane Policing 8
    Network-Based Application Recognition (NBAR) 9
    Autosecure 10
  Secure Connectivity 11
    Virtual Private Network (VPN) Encryption and Tunneling 12
    Dynamic Multipoint VPN (DMVPN) 12
    Voice and Video Enabled IPSec (V3PN) 13
    Secure Real-Time Transport Protocol (SRTP) 14
    Multi-Protocol Label Switching (MPLS) & IPSec Integration 14
  Threat Defense 16
    IOS Firewall 16
    Transparent Firewall 17
    Intrusion Prevention 17
  Security Certifications 18
    FIPS 18
    ICSA 18
    Common Critria 18
The Service-Provider Scenario 20
  An Overview of Dalriada Communications 20
  Network Infrastructure Hardening 21
  Attack Mitigation 24
Futures 27
Conclusion 29
References 30

List of Figures

Figure 1 The Router's Role in the Self-Defending Network 4
Figure 2 - NAC Architecture 5
Figure 3 - The Dalriada Communications Inc Infrastructure 20

Abstract/Summary

A number of years ago, Cisco initiated a strategy intended to achieve integrated security at the network level, called the Self-Defending Network and, during the past six months, Cisco has made announcements that have moved the company closer to their vision of a security-intelligent network.

The Self-Defending Network is a phased strategy with phase 3 being the latest. This paper focuses on Phase 2.

Phase 2 of the Self-Defending Network has been divided into four functional categories. These, and their component technologies, are listed below. The Self-Defending Network is aimed at the enterprise sector but its technologies are also applicable to the service-provider market in some form or another. This list below also contains a grading against Service Provider relevance for each technology.

Trust and Identity

• Network Admission Control	***LOW***
• Identity-Based Network Services	***LOW***
• Authentication, Authorization and Accounting	***HIGH***

Network Infrastructure Protection

• Control-Plane Policing	***HIGH***
• Network-Based Application Recognition	***MEDIUM***
• AutoSecure	***MEDIUM***

Secure Connectivity

• Virtual Private Networking	***HIGH***
• Dynamic Multipoint Secure Private Networking	***HIGH***
• Voice and Video Enabled IPSec (V3PN)	***MEDIUM***
• Secure Real-Time Transport Protocol (SRTP)	***LOW***
• MPLS and IPSec Integration	***MEDIUM***

Threat Defense

• IOS Firewall	***MEDIUM***
• Transparent Firewall	***LOW***
• Intrusion Prevention	***MEDIUM***

Introduction

The Cisco 'Self-Defending Network' strategy aims to bring security intelligence to the network by evolving Cisco's traditional core product set from mere routers and switches to network appliances containing integral security features.

In support of this, Cisco announced three new Integrated Services (IS) router models in late 2004; the 1800, 2800 and 3800 series. These, coupled with the existing security features of the 7200, 7301 and 7600 series routers, provide a network-based security architecture, intended to be the foundation of the Self-Defending Network.

Whereas security functions have been available on routers and switches for a number of years, IS routers evolve these through the inclusion of built-in hardware encryption, hardware options such as encryption, Intrusion Detection System (IDS) and Content Engines, and specific IOS feature sets that support solutions such as Dynamic Multipoint VPN, V3PN, VRF-Aware firewall and others.

The intention is that integrated, network-based security functions be made available to the Small to Medium Business (SMB) and large enterprise branch office, allowing this part of the network to participate in a coherent security strategy. However, as service-provider business models evolve to expand on managed service offerings, including multiservice (voice/video), web and application hosting, advanced VPN and security services, the division between the enterprise and the service-provider is becoming less distinct.

This paper examines the Self-Defending Network strategy and its relevance to the service-provider environment by describing each technology within the Self-Defending Network strategy and its applicability to the service provider. A fictitious scenario will also show how a service provider might utilize two of these technologies. Finally, Cisco's future strategy, announced in February 2005, will be discussed.

The Self-Defending Network

This chapter provides an overview of the Cisco Self-Defending network and the security functions of the IS Router.

Cisco's 'Self-Defending Network' is a phased approach to network security.

The first phase implemented security technology into network router products through the introduction of IOS VPN services, the IOS firewall and others.

The second phase, launched in late 2004, took this further by introducing Integrated Services Routers and enhancements to the Network Admission Control technology.

Phase-three [a], announced in February 2005, introduces the concept of Adaptive Threat Defense.

[1] Cisco Systems Inc. Charles Waltner "Cisco CEO Chambers Details Company's Vision for Network Security" Feb 22 2005 http://newsroom.cisco.com/dlls/2005/ts_022205.html

Phase one of the Self Defending Network strategy has been available for a number of years and is well documented This paper focuses on the phase-two technologies and, in particular, those associated with the new range of IS Routers, announced in October 2004. Phase three, announced in February 2005, is also covered, in the Futures section.

The Integrated Services Router

IS Routers provide security functionality that can be listed under four categories, namely:

- Trust and Identity
- Network Infrastructure Protection
- Secure Connectivity
- Threat Defense

A vague alignment can be made between these and the SANS Defense-in-Depth approach which mandates that a good security policy should include different facets of security. In effect, Cisco is attempting to apply the Defense-in-Depth philosophy to the network.

The table below shows a loose correlation between the Cisco security categories and the Defense-in-Depth principles of Confidentiality, Integrity and Availability (CIA).

Cisco	CIA
Trust and Identity	Integrity
Network Infrastructure Protection	Availability
Secure Connectivity	Confidentiality
Threat Defense	Availability

Table 1

Each category is served by security technologies, all of which are now available on the network IS router, or in which the IS router can participate, as shown on Figure 1 below.

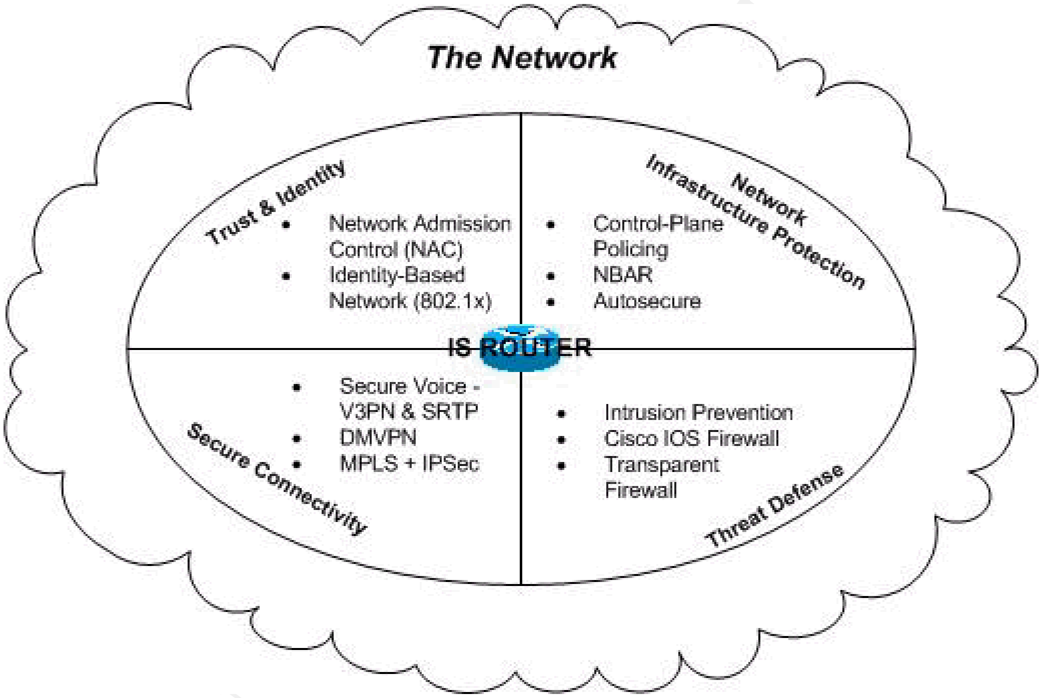

Figure 1 The Router's Role in the Self-Defending Network

IS Routers support these technologies through a combination of integrated security hardware, hardware modules and Cisco Internet Operating System (IOS) feature sets.

Headend routers (7200, 7301, 7600) support the same technologies though hardware modules and IOS feature sets.

The following sections describe Self-Defending Network technologies in more detail. All data is taken from:

[2] Cisco Systems Inc. “Network Security Features on the Cisco Integrated Services Routers” 2005
http://www.cisco.com/en/US/products/ps5854/products_data_sheet0900aecd80169b0a.html

Trust and Identity

This category aims to give the network the ability to control access at the endpoint, thus providing protection from end systems that connect to the network infrastructure. Contributing to this are Network Admission Control (NAC), IEEE802.1x and Authentication, Authorization and Accounting (AAA).

Network Admission Control (NAC)

NAC is an industry wide initiative, sponsored by Cisco, which enables the network to interrogate end-systems for compliance with a security policy.

It is designed to control initial network access, either by allowing, blocking or quarantining end systems. The access decision is made by referencing the end-system’s security posture (OS hardening, OS revision and patches, virus protection, etc) against a predefined security policy.

Obviously, such functionality requires more than just intelligent network elements. For this reason, NAC is a multi-vendor collaboration, involving representations from network, anti-virus, OS management and specialized security vendors. At the time of writing, Cisco, Computer Associates, IBM, McAfee, Symantec and Trend Micro are shipping NAC-enabled products, with eleven other vendors expecting to ship within ninety days [c].

[3] Cisco Systems Inc “Network Admission Control – Current Participants”
http://www.cisco.com/en/US/partners/pr46/nac/partners.html

A typical NAC architecture is shown in Fig 2.

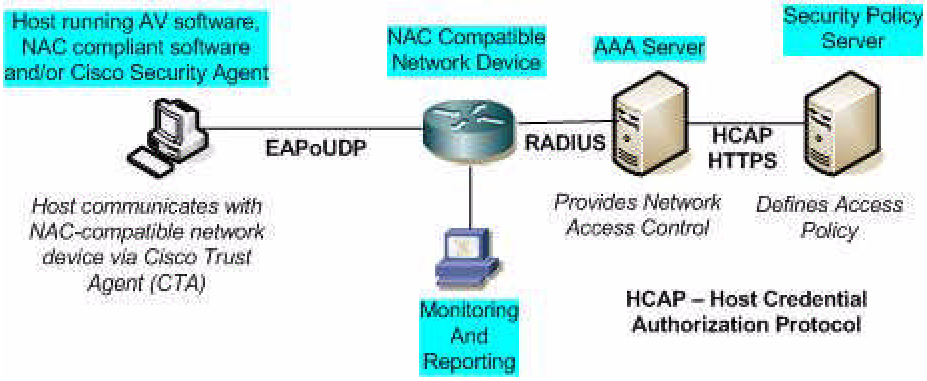
Host running AV software, NAC compliant software and/or Cisco Security Agent
NAC Compatible Network Device
AAA Server
Security Policy Server
EAPoUDP
RADIUS
HCAP HTTPS
Host communicates with NAC-compatible network device via Cisco Trust Agent (CTA)
Provides Network Access Control
Defines Access Policy
Monitoring And Reporting
HCAP – Host Credential Authorization Protocol

Figure 2 - NAC Architecture

When a end system connects to the network, it is checked for the presence of the Cisco Trust Agent (CTA). If CTA isn’t installed, the system will either be blocked or given restricted access. If CTA is present on the system, access will be requested from the AAA server which, in turn, will reference the security policy server to establish the access rights of the system. If the Security Policy Server confirms the system to be trusted, (e.g. appropriate anti-virus installed, OS patches up to date, etc), the AAA server will communicate this to the NAC-compatible network device, which will in turn allow access through a dynamic Access Control List (ACL). All of this can be done without intervention from a network or security administrator, although it would be prudent to enable alerting for non CTA end systems or systems that do not meet security policy.

The initial phases of NAC are supported on Cisco routers, giving access control at the IP level. The CTA on the end system communicates with the NAC router using Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP). While this will satisfy some security models, a fully-enable NAC network will need to control access at all types of network edge, including workgroup switch, network access server (NAS) and wireless access-point (AP). This requires authentication at layer 2 of the OSI model. EAPoUDP operates at layer 3 so, for future phases of NAC, an additional technology will be used for switches, APs, etc; IEEE802.1x with EAP.

Relevance to the Service Provider : ***LOW***
A SP may use this technology to control access to its own corporate network but is unlikely to make use of it on their customer networks as, typically, SP ownership ends at the customer-site presentation (router or cable). Only in certain managed services scenarios where the SP manages/provides the customer LAN/MAN or Remote-Access infrastructure and is able to install the CTA on end-systems, might this be offered as managed security option. Wireless and Remote Access support, when made available, may increase relevance to the SP.

Identity-Based Network Services - IEEE 802.1x

IBNS allows access control at a user port level. This means that users may be permitted or denied access to the network based on login credentials supplied.

Originally, network perimeter access control (as opposed to system or device access control, controlled by AAA) was available either by manually disabling switch ports or using MAC address criteria, where each switchport would only permit a specific MAC address to connect.

This is administratively cumbersome, so IBNS takes network authentication further by basing access control not on MAC address, but on user identification details. When an end system connects to a network, the layer two network device will ask the user to log in. The ID and password are sent to an authentication server (RADIUS/AAA) and checked against access policy. The end user is permitted or denied access to the network.

This is achieved by using IEEE802.1X as the underlying technology. 802.1X is a standard that enables end systems (known as *supplicants* in an 802.1X architecture), network elements (known as *authenticators*) and AAA servers (known as *authentication servers*) to communicate with each other, thus applying access policy to the network edge.

Cisco supports 802.1X in a number of edge products, including Secure Access Control Servers, Aironet Wireless, and Catalyst switches. Cisco has also made some enhancements to 802.1X to support particular networking technologies:

- VLAN Assignment – allows switches to dynamically assign a port to a VLAN based on user identity.
- Port Security – permits only one MAC address to connect to each port, so reducing the risk from other machines connecting via network hubs on switchports.
- Voice VLAN ID – provides supports for Cisco's Architecture for Voice, Video and Integrated Data (AVVID).
- Guest VLAN – assist with migration to 802.1X by allowing non-802.1X devices to connect to a switch, whereby they are place in a guest VLAN.
- High Availability – allows port security information to be synchronized by active and standby Catalyst supervisor cards to maintain port security state in the event of a supervisor failover.
- ACL Assignment – allows further control over user access. Certain users can be restricted to certain areas of the network by dynamically applying ACLs to control destination addresses or applications permitted.

While IBNS is more aligned towards Cisco's SAFE blueprint than the Self-Defending Network, there are strong similarities between it and NAC. Both control end system access to the network. Both use, (or will shortly), 802.1X for layer 2 access control. Both use AAA authentication servers. The primary difference between the two is that, where IBNS controls access based on user identity, NAC controls access based on the security posture of the accessing system, e.g. anti-virus software and OS patches.

At the moment, Layer 3 NAC is autonomous from end user Authentication, Authorization and Accounting (AAA), but as NAC moves to layer 2 and makes use of 802.1x, it will become integrated with IBNS services, providing access based on user identity AND end system security posture.

Relevance to the Service Provider : ***LOW***
Like NAC, this solution requires end-systems to support 802.1X authentication and, as such, may apply to a limited managed service offering or the SP's own internal network.

Authentication, Authorization and Accounting (AAA)

AAA provides the mechanism by which users are authenticated to a system, their access level set and their actions logged. The system in question may be an application, a physical resource such as a server or network device or a network infrastructure.

The most common AAA methods are Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System (TACACS+) and Kerberos. RADIUS is typically used to authenticate users who access a network via dial-up or xDSL. TACACS+ is often used to authenticate technical users within an enterprise, such as for access to network devices or network management systems. Kerberos is favored by application developers who may use it to establish authentication between users and elements in a multi-tiered application.

Cisco offers AAA services in its Secure Access Control Server (ACS) product.

AAA is a fundamental part of most organizations' security policies. Not only does it provide a standalone authentication method, it is also a component part of many access architectures, including one-time passwords (tokens) and IBNS. In the context of the Self-Defending Network, AAA is key as it is required for Network Access Control. The Cisco Trust Agent in a NAC-compliant end-user communicates with an AAA server which, in turn, requests security policy details from the policy server.

Relevance to the Service Provider : ***HIGH***
AAA is a core part of most SP's offerings. It is used to authenticate customers for network access as well as authenticating and monitoring internal access to certain systems.

Network Infrastructure Protection

The network supports IT services that, in turn, support business requirements. It also provides a platform for advanced security services, designed to protect those same IT services. However, if the network infrastructure should become compromised, both end systems and security mechanisms that rely on the network to function will be rendered ineffective.

For this reason, it is important that the network infrastructure be made as robust as possible. This is why Cisco's Self-Defending Network strategy has a category devoted to the protection of the network.

Control Plane Policing

One of the most common ways to disrupt or disable a network is though a Denial of Service (DoS) attack, where the infrastructure is overloaded by volumes of contrived, meaningless traffic. In many cases, network elements will discard real network traffic, trying to cope with what has been generated by the attack.

Cisco IOS software offers Control Plane Policing (CoPP) functionality, intended to protect the network against DoS and Distributed DoS attacks. As its name suggests, CoPP protects the control plane (and management plane), the functional component of a network element responsible for handling routing updates, keepalives and management traffic (management plane), all of which are requisite to the health of a network. Control plane and management plane traffic is generally that which originates from or is destined for a network element (as opposed to traffic which passes through a network element, commonly known as data plane traffic).

CoPP uses Cisco Modular Quality of Service (QoS) capabilities to rate-limit control plane traffic. This traffic policing is configurable to fit into a particular organization's security policies.

CoPP is supported in IS routers, 1700, 2600, 3700, 7200 and 7500 series routers.

Relevance to the Service Provider : ***HIGH***
CoPP is an effective way to harden the network infrastructure against attacks. This is particularly important for a SP as much of its network infrastructure is directly connected to the Internet. Therefore, it does not benefit from the protection provided by firewalls, and needs other forms of attack mitigation. By limiting the volume and types of traffic that can be sent to a network element, CoPP maintains the network robustness.

Network-Based Application Recognition (NBAR)

NBAR is also closely associated with Cisco QoS functionality in that it is used to classify traffic that can then be appropriately handled by QoS [d]. In this respect, NBAR can be thought of as an application classification engine, able to classify the following types of protocol:

- Statically assigned TCP and UDP port numbers
- Non UDP and non-TCP IP protocols
- Dynamically assigned TCP and UDP port numbers
- Sub-port classification through deep packet inspection

[4] Cisco Systems Inc "Network-Based Application Recognition IOS 12.2T" http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cd0.html

In this way, it is possible to configure routers to rate limit and prioritize specific applications, not recognizable through standard IOS ACLs and QoS. When enabled, NBAR will monitor traffic at the OSI layer 4 to layer 7 level and classify it against a predefined list of applications. Anything not recognized is recorded as 'unclassified'.

The NBAR classification engine can also be used to detect worm and virus signatures at a network level through the use of custom application designation which allows new protocols or traffic signatures to be added to NBAR and Custom Packet Description Language Modules (PDLM), which are written to recognize specific applications and attack signatures and are downloadable from the Cisco website.

Relevance to the Service Provider : ***MEDIUM***
One of an SP's greatest challenges is to control self-propagating attacks, such as worms. NBAR has the potential to help with this by giving the network the ability to recognize and react to attack signatures. However, such functionality requires processing power and it is unclear at this time how existing infrastructure routers might cope with the deep-packet analysis requirements of NBAR. For this reason, relevance is marked as MEDIUM. See the Service-Provider Scenario section for more details.

Autosecure

Autosecure is simply the automation of router IOS security configuration best practices, as recommended by Cisco and the National Security Agency [e]. Autosecure affects only the router on which it is run; to lock down all routers in a network infrastructure, it is necessary to run Autosecure in each router. This feature was first introduced in IOS version 12.3(1).

[5] National Security Agency "Router Security Configuration Guide" Dec 2003
http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf

Autosecure can be invoked within the IOS CLI by running the auto secure command in privileged mode. A number of options are offered:

- Management – only the management plane of the router is secured –
    - Disable often unnecessary global services such as finger, chargen, echo, HTTP
    - Disable often unnecessary per-interface services such as proxy-arp, icmp-redirects, icmp-unreachable messages, icmp-mask-reply messages.
    - Enable global security services such as password encryption, TCP synwait time, TCP keepalives
    - Secure router access by prompting for a login banner, enabling SSH and SCP (if supported by IOS) and applying passwords to AUX, CON and TTY lines.
    - Disable SNMP if not required

    - Configure logging for security
- Forwarding – only the forwarding plane of the router is secured
    - Enable Cisco Express Forwarding to perform better against SYN attacks.
    - Activate the IOS firewall (where the router is running an image that supports firewall) and offer the option to enable Context-Based Access Control (CBAC)
    - Activate anti-spoofing using Unicast Reverse-Path Forwarding (uRPF) if available on all public interfaces.
    - Create ACLs to block addresses from the RFC1918 (public IP) [f] and bogon (not yet assigned by IANA) address spaces [g].

[6] Internet Engineering Task Force - Rekhter/Moskowitz/Karrenberg/de Groot/Lear "RFC 1918 – Address Allocation for Private Internets" Feb 1996
http://www.ietf.org/rfc/rfc1918.txt?number=1918

[7] Internet Assigned Numbers Authority "Internet Protocol V4 Address Space" Jan 2005
http://www.iana.org/assignments/ipv4-address-space

Both the uRPF and ACL options are intended to combat IP address spoofing, where an attacker will forge the source address of attack packets to either hide his identity or cause end stations to send spurious response packets to the subject of the attack. RFC1918 and bogon ACLs are usually used at Internet facing interfaces, where these sources should never be seen. However, this approach does not work for interfaces that legitimately connect to RFC 1918 addresses, (such as an SP's customers). In these cases, uRPF may be used, where traffic received on an interface will not be forwarded unless the source address is present in the router's IP routing table. NOTE that uRPF may not work where asymmetric routing is in effect, such as for dual-homed sites. Strategies to defeat address spoofing at the network level are discussed in RFC 2827 [h].

[8] Internet Engineering Task Force - Ferguson/Senie "RFC 2827 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" May 2000
http://www.ietf.org/rfc/rfc2827.txt?number=2827

Either or both Management and Forwarding options can be applied to Autosecure and both can be run in either full mode, where the user is prompted for all interactive configurations or no-interact mode, where the user is not prompted for interactive configurations.

Relevance to the Service Provider : ***MEDIUM***
All network elements must be hardened and AutoSecure can help to achieve this. However, care should be taken to ensure AutoSecure doesn't interfere with the normal operation of the network. In certain cases, it may be safer to manually harden the router, for example where asymmetric routing conditions

exist, as in multi-homed customer connections, it is not prudent to use uRPF. See the Service-Provider Scenario section for more details.

Secure Connectivity

It should be possible for the network to pass data in a manner that renders it secure. However, the methods used to secure data on the network should also be scalable. The Secure Connectivity category provides mechanisms to achieve this.

Virtual Private Network (VPN) Encryption and Tunneling

VPN encryption is the traditional method of encrypting traffic between network sites, or from remote users to the network edge. One of the most common methods to achieve this is by using the IPSec architecture to negotiate encryption keys (using Diffie-Hellman and RSA), authenticate data (using SHA-1 or MD5) and encrypt data (using DES, 3DES, or AES). Cisco provides IPSec acceleration through hardware-based encryption in a number of its products, either through integrated hardware (as in the case of Integrated Services Routers) or optional encryption modules. Cisco's VPN encryption module also supports IP Payload Compression Protocol (IPPCP).

In addition to standard IPSec, Cisco also exclusively supports IPSec with Generic Routing Encapsulation (GRE) tunneling. Traditional IPSec encrypts traffic defined by IP address and/or protocol. This allows a high level of control over which traffic is eligible for encryption. However, IPSec will only encrypt IP unicast traffic, traffic destined for a single IP address, thus precluding non-IP protocols, IP routing protocols and IP Multicast.

An alternative is to build a GRE tunnel between two points on the network and encrypting all traffic flowing across it. As a GRE tunnel encapsulates traffic in unicast IP, it is possible to encrypt non-IP protocols and IP multicast/broadcast packets, such as used by IP routing protocols.

<u>Relevance to the Service Provider :</u> ***HIGH***
VPNs are an important part of many SP's product offerings and are also used for a number of internal functions. GRE Tunnelling with IPSec may be less of a requirement as customer solutions that need to carry routing updates, multicast, etc. are usually provided by the SPs private WAN network. However, Tier 2 SPs may make use of it to broaden their product offerings.

Dynamic Multipoint VPN (DMVPN)

IPSec uses a point-to-point model, in that an IPSec VPN is setup between two points on a network, such as across the Internet or from a remote location to a central office.

This works well for hub and spoke topologies where most traffic flows to and from a central location. However, in such topologies, where some communication between spokes is also required, traffic must flow to the hub, be de-encrypted, be re-encrypted and sent to the destination spoke. To avoid this, (or having to configure a full mesh of IPSec VPNs), DMVPN can be used. This technology allows for static VPNs between spokes and hub, and dynamic VPNs between spokes that require direct connectivity. DMVPN uses multihop GRE and Next-Hop Resolution Protocol (NHRP) to resolve peer destination address and automate IPSec encryption initiation, i.e. the establishment of Security Associations (SAs).

NOTE that DMVPN is intended as an enhancement to hub and spoke topologies where some spoke-to-spoke connectivity is required. For large fully meshed configurations, an alternative configuration technology should be considered, such as On-Demand VPN with Tunnel Endpoint Discovery.

Relevance to the Service Provider : ***HIGH***
A SP that offers IPSec-based VPN products could greatly enhance its offerings through the application of DMVPN, in some cases using the Internet to compete with large SP Private WAN offerings.

Voice and Video Enabled IPSec (V3PN)

V3PN provides a solution to the problem of supporting voice, video and data services across a secure network path. It combines Cisco's IP Telephony, VPN and QoS technologies to create network models for site-to-site, small office / home office (SOHO) and remote access topologies.

The present IPSec VPN model provides a strong business case for many organizations to transmit data over public network topologies in a secure and cost-effective manner. However voice and video applications rely on strict network performance criteria; the Cisco Powered Network Multiservice Service Provider designation [i] specifies that a service provider guarantee end-to-end metrics of:

- Latency <= 150 ms
- Jitter <= 30ms
- Packet Loss <= 1%

[9] Cisco Systems Inc. "Cisco Powered Network Program – Eligibility and Requirements" http://www.cisco.com/en/US/applicat/cpnapply/applications_user_agreement.html

In a non-encrypted network, traffic is prioritized according to settings in the IP packet Type of Service (ToS) field, either IP Precedence or Differentiated Services Code Point (DSCP). Because IPSec Tunnel Mode encapsulates the original packet, including the IP header, these classifications are also encrypted meaning that all traffic across an IPSec connection is treated the same. This is unacceptable for Voice and Video which need to be prioritized over data to meet their performance requirements.

V3PN provides the functionality to apply QoS across an IPSec connection. This, in turn, means that VPN applications such as SOHO or telecommuting can now also use their IPSec VPNs for voice services as well as data.

Relevance to the Service Provider : ***MEDIUM***
SPs are keen to offer Voice and Video services but will usually do so across the private network infrastructures, where encryption is not usually a requirement. However, where the customer does require encryption or where the provider is Internet-based, V3PN will enable voice and video services to be encrypted and prioritized across the public network..

Secure Real-Time Transport Protocol (SRTP)

RTP is the IP-UDP protocol used to transport voice conversations (among other things). SRTP is an IETF standard that provides the end-to-end encryption of voice calls. SRTP supports the AES-128 encryption standard (Advanced Encryption Standard).

Where IPSec would normally encrypt a call in a tunnel that spans part of the network, SRTP encrypts the call end-to-end, from IP phone to IP phone. Also, because SRTP only encrypts the payload of the voice call packet, it is more efficient than IPSec.

These may seem like strong arguments for SRTP over IPSec but the network topology should be taken into account before any decision is made. Because SRTP only encrypts the payload, the source and destination addresses of the call are visible to anyone who can capture the packet stream and this is valuable information for an attacker.

If the encryption is required to protect call content and the network infrastructure is trusted end-to-end, then SRTP is a valid option. If, however, any part of the network path is not trusted, such as a Service Provider WAN or the Internet, then a V3PN IPSec tunnel should used to protect the identity of the end devices.

Bear in mind that V3PN and SRTP can complement each other. SRTP can encrypt on the LAN/MAN portions of the call path while V3PN can protect the call across non-trusted domains.

Relevance to the Service Provider : ***LOW***

Because of its end-to-end nature SRTP is more likely to be used in the enterprise. SPs are not expected to make use of SRTP except where specific configurations require end-to-end encryption and the SP has access to or can influence the configuration of the end devices, as in a managed IP Telephony solution.

Multi-Protocol Label Switching (MPLS) & IPSec Integration

Service providers have adopted MPLS as a backbone technology that allows them to offer IP-based QoS services and to carry multiple customers' connections across a single core infrastructure using IPVPN functionality of MPLS.

These VPNs only reach from one edge of the core MPLS network to the other and because they exist on a private WAN network, are typically not encrypted. The connections from the MPLS edge to the customers' premises is usually achieved through dedicated network infrastructure, that is, separated from other customers by hardware which negates the requirement for VPN services.

However, Many organizations now use IPSec to encrypt all traffic that leaves their own network domains which, in the case of connectivity provided by an MPLS service provider, would require that the customer premise to MPLS edge connection be encrypted. Also, many providers wish to extend VPN services across partner or public networks.

The Self-Defending Network provides the capability to map IPSec sessions into MPLS VPNs, so allowing the VPN to be extended across non-trusted networks.

An alternative approach to this can be applied when the MPLS edge to customer network is trusted (belongs to the same provider as the core) but VPNs must be extended into the customer's network. VRFLite (also known as Multi-VPN Routing and Forwarding (VRF)) allows MPLS VPNs to be extended from the MPLS edge into a customer router which will run multiple VRFs. Because MPLS VPNs are typically not encrypted, (as VPN distinction is made through Route Designators and Route Targets), this option is only really applicable when the site-to-site connection is owned by the a single organization, such as a service provider.

Another common application of VRFLite, is to extend IPVPNs past the Provider Edge (PE) device to a switch which can then be used as an aggregator. However, this is usually done for efficiency reasons (switchports may be cheaper than router ports) rather than for security reasons.

Relevance to the Service Provider : ***MEDIUM***
Again, MPLS SPs typically use secure transport methods for their cusctomer access methods, such as leased line, ATM, xSDL, etc. However, MPLS/IPSec

integration may add Internet VPNs to the possible access methods, so increasing the SPs potential service footprint. For example, a company who uses a SPs MPLS network to provide inter-office connectivity, could extend that connectivity to its home workers and business partners across IPSec VPNs. Used in conjunction with V3PN, the MPLS QoS offering could also be extended across the IPSec VPN for voice and video applications

.

Threat Defense

This category provides ways in which the network can prevent and respond to attacks.

IOS Firewall

The Cisco Advanced Security IOS feature sets (formerly known as the IOS Firewall feature sets) provide IOS firewall functionality. Essentially, this is a stateful firewall that runs in a Cisco router. IOS firewall runs in software so is limited by the processing capacity of the host router. For this reason, IOS firewall is intended for use at network edge points where traffic volumes are conservative, such as SOHO implementations.

IOS firewall has been enhanced to provide specific functionality:

- Advanced Application Inspection and Control – this allows the firewall to inspect HTTP traffic to prevent attacks such as port80 tunneling, where rogue applications use port 80 in an attempt to pass through the firewall, Trojans, where malicious code is embedded within HTTTP traffic, and malformed packets, where HTTP packets are altered (e.g. TCP flag changes) to disrupt end systems. Email inspection is also supported to prevent misuse of email connectivity and protocol masquerading.
- VFR-Aware Firewall – Virtual Routing and Forwarding instances are used at the edge of MPLS networks. This allows a label-edge router to be logically divided into a number of 'virtual' routers. IOS firewall has the ability to recognize each VRF in a router and apply rule context appropriately.
- H.323 Support – the firewall can permit H.323 channels, some of which are opened from the H.323 client side (as in the H.323 V2 client) using dynamic port allocation.

For higher performance protection, the self-defending network also offers the Firewall Services Module (FWSM), a Catalyst 6500 and 7600 router linecard that provides hardware-based firewall services in existing network infrastructure for protection of headends and data centers. For situations where dedicated firewalls are required, the PIX firewall, a standalone firewall appliance, is also available.

Relevance to the Service Provider : ***MEDIUM***
A SP would normally make use of dedicated firewalls (such as PIX or Checkpoint). However, IOS firewalls could form part of a managed security services solution, particularly for managed customers with onsite SP owned routers.

Transparent Firewall

A number of Cisco routers support transparent firewall. This is the ability to provide a OSI Layer 3 firewall for Layer 2 connectivity. A firewall can be placed in a Layer 2 infrastructure (e.g. where a wireless access-point connects to a LAN switch) and can filter traffic based on IP address, ports and other Layer 3 criteria even though the traffic remains on the same LAN segment. The Transparent Firewall understands VLANs, subinterfaces, spanning tree Bridge-Protocol Data Units (BPDU) and DHCP traffic. It can be installed in a network without adding IP addresses to its interfaces and the network requires no re-addressing.

Relevance to the Service Provider : ***LOW***
A SP is unlikely to make use of this functionality, except for very specific, ad-hoc solutions. One of these may be a wireless infrastructure.

Intrusion Prevention

IOS Intrusion Prevention is the evolution of Cisco's IOS IDS. As of IOS release 12.3(8)T, released in June 2004, IOS IDS has been enhanced and renamed IOS IPS. Like IOS Firewall, IOS IPS runs in software on the router, so providing an inline IPS system capable of signature analysis that enables the router with the ability to drop traffic, generate alarms, shun traffic or reset connections.

Used in conjunction with IOS firewall, the IPS can scan for signatures only on traffic that has been permitted by the firewall. It contains a number of built-in signatures (132 in IOS 12.3(8)T) which are held in a Signature Definition File (SDF), an XML file residing on the router flash or a remote server. IOS IPS supports more than 740 signatures but the number of signatures that can be loaded depends on the amount of memory available in the host router. For IS routers, up to 563 signatures can be loaded on platforms with 128MB of memory; 737 signatures can be loaded when there is 256MB of memory.

IOS IPS uses the concept of parallel scanning to increase the efficiency of the scanning engine but, even so, cognizance must be taken of the processing limitations of the host router. Deployment of IOS IPS requires careful placement and an understanding of the types of traffic likely to pass through the router.

Other Intrusion Detection/Prevention products available from Cisco include IPS 4200 series sensors, Catalyst 6500 IDS Services Module (IDSM-2) and the IDS module for Cisco Access Routers.

<u>*Relevance to the Service Provider :*</u> ***MEDIUM***
As with IOS firewall. this may form part of a managed security solution at the edge but is unlikely to be used in the core infrastructure.

Security Certifications

Cisco has attained security certification for a number of its products [j].

[10] Cisco Systems Inc. “Cisco Security & VPN Certification/Evaluation” http://www.cisco.com/go/securitycert

FIPS

7200 series routers and 7600 VXR routers with the VPN services module have achieved Federal Information Processing Standard (FIPS) 140-2 validation, “Security Requirements for Cryptographic Modules”. The IS Router models (1800, 2800, 3800) are undergoing FIPS 140 -2 validation with an estimated completion time of Q1 2005. FIPS are standards developed by the National Institute of Standards and Technology (NIST) for use in United States federal computer system. Therefore, FIPS validations are important for government installations. In particular, the FIPS 140-2 document states that,

> “This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. “

This means that FIPS 140-2 is mandatory for any cryptographic devices used by government agencies, except where the device in question has alternatively been approved for classified use.

NOTE that FIPS do not apply to National Security Systems.

ICSA

IOS Firewall has attained ICSA Certified Firewall status against version 4.1 of its certification criteria [k]. ICSO certification is aimed at the commercial sector, allowing prospective clients to identify products that have been independently certified against industry-accepted standards.

[11] ICSA Labs "4.x Certified Firewall Products" Oct 2004 http://www.icsalabs.com/html/communities/firewalls/newsite/cert2.shtml

Common Critria

Common Criteria Evaluation Assurance Level (EAL)2, 3 and 4 evaluations for IOS firewall, IOS VPN, a range of routers (including IS routers), Catalyst switches and other Cisco products is ongoing with completion expected in 2005.

Common criteria represent an international set of evaluation criteria and standards for security technology. It is important for international acceptance of a product.

The Service-Provider Scenario

Now that we have reviewed the component parts of the Self-Defending network, we will examine how the strategy might be used in a service-provider environment. To this end, consider the case of a fictitious provider, Dalriada Communications Inc.

An Overview of Dalriada Communications

Dalriada is a Tier 1 service-provider, providing Internet access services to a number of Tier 2 ISPs and corporate customers. It also provides broadband Internet services to the consumer market and managed connectivity solutions to the corporate market. It has an MPLS core infrastructure configured with Quality of Service features which, it hopes, will help to support a number of planned managed services offerings such as hosting, multiservice (voice/video) and security.

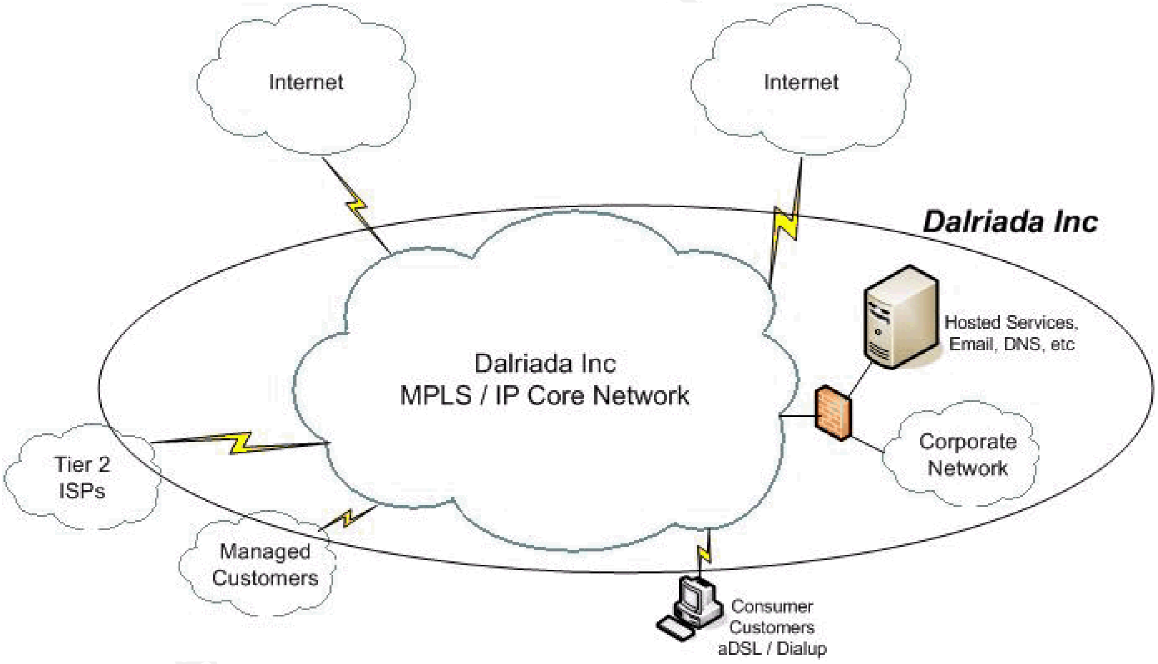

Figure 3 - The Dalriada Communications Inc Infrastructure

As well as a strategic intention to become a Managed Security Services Provider (MSSP), recent worm activity and distributed DoS attacks have put Dalriada under some pressure to improve the security of the services they currently provide, particularly in relation to those that give Internet connectivity.

In response to this, Dalriada has reviewed their security policy in the context of the SANS Defense-in-Depth principles and RFC3013 – Recommended Internet Service Provider Security Services and Procedures [l]. A number of actions have arisen out of the review and Dalriada has defined a subset of these that, they believe, can be satisfied at the network level:

- Network Infrastructure Hardening using Autosecure and specific filtering
- Attack mitigation using NBAR and TCP Intercept.

The following assumes that Dalriada has previously conducted an analysis of installed hardware and IOS code versions to ensure that the existing infrastructure can support the proposed changes.

Network Infrastructure Hardening

Section 4 of RFC3013 states that "ISPs are responsible for managing the network infrastructure of the Internet in such a way that it is reasonably resistant to known security vulnerabilities and not easily hijacked by attackers for use in subsequent attacks."

Dalriada has already implemented AAA on all routers to control access but router configurations have not been standardized. Dalriada harden all their network routers and apply filtering both at Internet peering points with other autonomous systems and at customer boundaries, either on the managed customer router or, in the case of xDSL or dialup customers, at strategic aggregation points.

Dalriada tests Auto Secure in the lab and decides to use management plane mode only for global application:

```
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
```

[12] Internet Engineering Task Force Killalea "RFC 3013 – Recommended Internet Service Provider Security Services and Procedures" Nov 2000 http://www.ietf.org/rfc/rfc3013.txt?number=3013

```
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport *

Configure SSH server? [yes]:
Enter the domain-name:dalriada.net

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 Disabling mop on Ethernet interfaces
```

* Because the routers are already configured for AAA authentication via TACACS+ then local ID, Auto Secure only configures AAA on routers where this configuration has been missed.

Dalriada manages its network devices via SNMPv2c over dedicated, out-of-band connections. Therefore Dalriada does not disable SNMP via autosecure but, instead, ensures that SNMP is blocked from all interfaces except the management one.

Forwarding Plane mode is not used because:

1. Auto Secure Forwarding Plane mode enables unicast RPF but Dalriada has a policy to not use uRPF on Internet peering points or multi-homed customers because of potential issues caused by asymmetric routing.
2. To maintain performance, Dalriada only wishes to apply anti-spoofing controls at the network edge, not on internal routers (i.e. without a direct connection to the Internet or a customer). Also, in addition to RFC1918, bogon and other illegal source addresses (loopback, multicast), Dalriada also wants to block ingress traffic at Internet peering points with source addresses of Dalriada's own address space.

Therefore, Dalriada manually applies the following access list inbound at all Internet peering points :

```
access-list 100 deny   ip 0.0.0.0 1.255.255.255 any
access-list 100 deny   ip 2.0.0.0 0.255.255.255 any
access-list 100 deny   ip 5.0.0.0 0.255.255.255 any
access-list 100 deny   ip 7.0.0.0 0.255.255.255 any
access-list 100 deny   ip 10.0.0.0 0.255.255.255 any
access-list 100 deny   ip 23.0.0.0 0.255.255.255 any
access-list 100 deny   ip 27.0.0.0 0.255.255.255 any
access-list 100 deny   ip 31.0.0.0 0.255.255.255 any
```

```
access-list 100 deny   ip 36.0.0.0 1.255.255.255 any
access-list 100 deny   ip 39.0.0.0 0.255.255.255 any
access-list 100 deny   ip 41.0.0.0 0.255.255.255 any
access-list 100 deny   ip 42.0.0.0 0.255.255.255 any
access-list 100 deny   ip 49.0.0.0 0.255.255.255 any
access-list 100 deny   ip 50.0.0.0 0.255.255.255 any
access-list 100 deny   ip 73.0.0.0 0.255.255.255 any
access-list 100 deny   ip 74.0.0.0 0.255.255.255 any
access-list 100 deny   ip 75.0.0.0 0.255.255.255 any
access-list 100 deny   ip 76.0.0.0 0.255.255.255 any
access-list 100 deny   ip 77.0.0.0 0.255.255.255 any
access-list 100 deny   ip 78.0.0.0 0.255.255.255 any
access-list 100 deny   ip 79.0.0.0 0.255.255.255 any
access-list 100 deny   ip 89.0.0.0 0.255.255.255 any
access-list 100 deny   ip 90.0.0.0 1.255.255.255 any
access-list 100 deny   ip 92.0.0.0 3.255.255.255 any
access-list 100 deny   ip 96.0.0.0 15.255.255.255 any
access-list 100 deny   ip 112.0.0.0 7.255.255.255 any
access-list 100 deny   ip 120.0.0.0 3.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 deny   ip 169.254.0.0 0.0.255.255 any
access-list 100 deny   ip 172.16.0.0 0.15.255.255 any
access-list 100 deny   ip 173.0.0.0 0.255.255.255 any
access-list 100 deny   ip 174.0.0.0 1.255.255.255 any
access-list 100 deny   ip 176.0.0.0 7.255.255.255 any
access-list 100 deny   ip 184.0.0.0 3.255.255.255 any
access-list 100 deny   ip 189.0.0.0 0.255.255.255 any
access-list 100 deny   ip 190.0.0.0 0.255.255.255 any
access-list 100 deny   ip 192.0.2.0 0.0.0.255 any
access-list 100 deny   ip 192.168.0.0 0.0.255.255 any
access-list 100 deny   ip 197.0.0.0 0.255.255.255 any
access-list 100 deny   ip 198.18.0.0 0.1.255.255 any
access-list 100 deny   ip 223.0.0.0 0.255.255.255 any
access-list 100 deny   ip 224.0.0.0 31.255.255.255 any
access-list 100 deny   ip d.d.d.d s.s.s.s any
access-list 100 deny   255 any any
access-list 100 deny   0 any any
access-list 100 deny   icmp any any fragments
access-list 100 permit tcp host n.n.n.n eq bgp host n.n.n.n  established
access-list 100 permit tcp hosts n.n.n.n host n.n.n.n eq bgp
access-list 100 permit tcp host n.n.n.n eq bgp host n.n.n.n established
access-list 100 permit tcp host n.n.n.n host n.n.n.n eq bgp
access-list 100 permit icmp any host n.n.n.n echo
access-list 100 permit icmp any host n.n.n.n echo-reply
access-list 100 deny   ip any host n.n.n.n
access-list 100 permit ip any any
```

The list above denies RFC1918, bogon loopback and multicast addresses, packets with source addresses that belong to the Dalriada assigned ranges (d.d.d.d s.s.s.s), protocol 0 (IPv6), protocol 255 (IANA reserved), permits BGP connections only to and from valid Internet peers (n.n.n.n), permits pings to the router and denies all other traffic to the router from the Internet.

At aggregation routers that connect to broadband and dialup Internet customers, Cisco Express Forwarding (CEF) and then uRPF are applied to allow only traffic with source addresses that exists in the aggregation routers' routing tables. At customer premises routers for managed customers, where many are multi-homed, the following is applied inbound on the customer-facing interface:

```
access-list 100 permit    ip  c.c.c.c s.s.s.s any
access-list 110 deny      any any
```

This allows traffic from the customer address space (c.c.c.c) but denies everything else which means that Dalriada's customers cannot, either intentionally or unwittingly, (as in the case of worms and bots) spoof traffic to the Internet or other Dalriada Customers. RFC3013, Section 4.4 recommends that traffic from the Internet to the Customer should be filtered to prevent source addresses that belong to the customer. Many providers choose to do this at point closest to their customers (e.g. aggregation routers or customer premises equipment) but Dalriada's decision to implement ingress filtering at Internet peer points which blocks sources that are assigned to Dalriada, effectively does the same thing.

To further harden the infrastructure, prefix lists are used to block illegal routing updates, so that the infrastructure routers will not learn about illegal networks. Control Plane Policing (CoPP) is applied to core routers to protect the infrastructure routing protocols against attack.

Attack Mitigation

Now that the network infrastructure has been hardened to reduce the risk of attacks directed at network elements and attacks using spoofed packets, Dalriada needs to consider their duty with respect to other attack types.

Dalriada requires a way to react to distributed and self-propagating attacks, such as DDoS and worms. They already have appliance-based IDS and firewalls to guard their corporate network but no way of controlling traffic flowing between their customers and the Internet. Such traffic flows across Dalriada's infrastructure without passing across a firewall or any form of intrusion prevention.

Dalriada identifies NBAR as a means to identify traffic from layer 4 to later 7 of the OSI model and decides to drop identified attacks at their aggregation routers, i.e. the points where multiple customers connect to the core network. This point is chosen against Internet peering points to distribute the load of scanning traffic. To prevent infection, traffic from Internet to customer is dropped at the aggregation routers. To prevent spread of attack, it is also dropped at the aggregation router as it leaves a customer.

NOTE that NBAR is not supported on Etherchannel, Tunnelling/Encryption, Dialer or Multilink PPP interfaces. Additionally, It is supported on VLAN interfaces but in the software switching patch only.

On each router, a class-map is configured. This will contain classifications for different attack types:

```
class-map match-any attacks
  match protocol mysql_udf_worm
  match protocol http url “*default.ida”
```

The NBAR Match Protocol and Custom features are used to define attack signatures. These signatures are taken from the Current Activity in the US-CERT site, http://www.us-cert.gov/current/ . For example, the MySQL UDF worm scans for systems using TCP port 3306, so it has been added to the class map using the following command:

```
ip nbar custom mysql_udf_worm destination tcp 3306
```

Similarly, the Code Red worm performs an HTTP GET for a file with a .ida extension. It has been added to the class-map using the following command:

```
match protocol http url “*default.ida”
```

In this way, as new attacks are identified, they can be added to the ‘block-attacks’ class map. This will significantly improve the network’s resilience to attack, although the appropriate end-system patches and other mitigation measures should also be applied.

The next step is to define an action for the identified attacks, using a policy-map:

```
policy-map  drop-attacks
    class attacks
       police 1000000 31250 31250 conform-action drop exceed-action drop
```

Traffic policing has been used as it is the most scalable solution, relying on neither Policy-Based Routing nor ACLs to drop the attack traffic. Note that the bits per second and burst rate quotes (1000000 31250 31250) are academic since both the conform and exceed actions are to drop the traffic. In effect, this means that any traffic which matches the criteria set out in the ‘attacks’ class-map will be dropped.

Finally, the policy-map is applied inbound to the interfaces facing the customer and the Internet on the aggregation routers:

```
interface FastEthernet 3/0
```

```
  service-policy input drop-attacks
interface GigabitEthernet 5/1
  service-policy input drop-attacks
```

So a sample NBAR-based attack mitigation configuration on each aggregation router is:

```
ip nbar custom mysql_udf_worm destination tcp 3306
!
class-map match-any attacks
  match protocol mysql_udf_worm
  match protocol http url "*default.ida"
!
policy-map  drop-attacks
    class attacks
       Police 1000000 31250 31250 conform-action drop exceed-action drop
!
interface FastEthernet 3/0
  service-policy input drop-attacks
interface GigabitEthernet 5/1
  service-policy input drop-attacks
```

As part of Dalriada's Defense-in-Depth approach to network security, they also implement Cisco's TCP Intercept at the network edge; Customer aggregation routers.

TCP Intercept reduces the effect of TCP SYN-flood attacks, where the attacker will bombard the target with TCP SYN requests. These attacks are usually spoofed with illegal source addresses and, as such, would be blocked by the filtering added in the Network Infrastructure Hardening section above. However, in cases where the spoofed sources are legal addresses or where the originator(s) are bots or zombies (end-systems that have been unknowingly compromised and used as part of an attack), the ACLs would not prevent the attack.

When configured, TCP Intercept intercepts the TCP SYN packet and establishes a connection with the source on behalf of the target. It then attempts to establish a connection with the target and, if successful, joins the connections together. If, however, the connection is spurious, the router will prevent further SYN requests from reaching the target system.

TCP Intercept allows for all connections to be intercepted, or only those for from or to particular addresses or network. Dalriada chooses to intercept all SYN packets to and from its own customers, on its customer aggregation routers. TCP Intercept is not configured on Internet peers because SYNs from the Internet, destined for Dalrida's own internal systems (such as web portals) are already protected by the anti-DoS mechanisms in their corporate firewalls. The TCP Intercept configuration looks like:

```
Access-list 110 permit any any
!
Ip tcp intercept list 110
```

Futures

Phase 3 of Cisco's Self-Defending Network strategy was launched in February 2005. It included a number of new products and guiding comment on Cisco's network security strategy.

Cisco believes that the scope of network security is changing and that the tenets of security must also change. It cites four main areas of change:

- The network perimeter is no longer easily defined, due to changing business requirements such as business partnerships, home working, and mobility. Technologies such as VPN and wireless make it more difficult to strictly control who might connect to a network.
- Ecommerce has collapsed network communications into a few, widely used protocols, such as HTTP and HTTPS. This makes it more difficult to block traffic at the network edge using traditional layer four ports for reference. Packet payload analysis is becoming more important as a tool against attackers.
- Virus and Worm development and propagation has accelerated to a point where manual mitigation will not control outbreaks.
- Regulatory Compliance such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act place pressure on organizations to secure data and provide robust forensics.

Cisco's intention for the evolution of the Self-Defending Network is an architecture that will contain inherent security intelligence, allowing it to identify and react to vulnerabilities and attacks. Cisco refers to this as adaptive defense, as opposed to the more traditional approach of proactive defense.

To illustrate this concept, Cisco makes a comparison with the human body's immune system, which can control the effect of external contaminants such as viruses, which enter the body every day.

At the moment, the network tries to block all potential sources of attack, a bit like a body with no immune system that must exist inside a plastic bubble. But the body must be liberated from the bubble, using its immune system for protection. This is what adaptive defense aims to do for the network.

This is the third phase of the Self-Defending Network. The first was Integrated Security, adding security functionality into network elements; the second, Collaborative Security, expanded this functionality and built security links between network and endpoints, as in the case of NAC; the third is referred to as Adaptive Threat Defense (ATD) and concerns itself with increasing network intelligence to respond to threats.

For Phase three, Cisco has redefined the Self-Defending Network building blocks.

- Endpoint Protection is Host-Based Intrusion Prevention through the Cisco Security Agent, resident on end systems. This is intended to be the first-order dampener of virus and worm propagation.
- Admission Control is an automated solution to control physical access to the network based on the security posture of the host (NAC), i.e. software patch levels and anti-virus capabilities. This should be the second-order dampener of virus and worm propagation.
- Infection Containment aims to use information from multiple sources to identify potential sources of attack. This is an improvement of network intelligence and considered as the third-order dampener of virus and worm propagation.
- Intelligent Correlation and Incident Response is Cisco's approach to Security Information Management (SIM). To achieve this, Cisco has acquired the MARS family of products from Protego Networks.
- Inline IDS and Anomaly Detection is actually an inline Intrusion Prevention System, available in the network through Integrated Security routers, hardware modules and standalone appliances.
- Application Security and Anti-X defense consists of technology that enables application inspection on the network to combat attacks such as SPAM, phishing, and spy-ware. The idea is that the network should have the ability to react to as many different types of attack with as little manual intervention as possible, hence the Anti-X name.

Conclusion

As attacks become more sophisticated and attack vectors become more diverse, it is clear that IT infrastructures must be in a position to defend and react against these more effectively.

This applies to both the enterprise and service provider environments.

Cisco views the network as a core element in infrastructure security and has articulated this philosophy through their Self-Defending Network strategy.

Although the strategy has been aimed primarily at the enterprise market, many of the component technologies are equally applicable to the service provider space and service providers should exercise the same (if not more) due diligence in securing their network infrastructures using such technologies to apply industry best practice and satisfy regulatory requirements.

Cisco's recent product announcements have brought more security functionality to the network but, in order for their vision of adaptive defense, the immune-system network, to be realized, network devices must change to incorporate security features as standard, not as add-ons, and not with a performance cost.

The Integrated-Services routers series have begun this change, incorporating IPSec processing in hardware as standard. However, there is still a long way to go. Network devices must be manufactured to be part of a larger security infrastructure, with internal processing capabilities to cope with the demands of encryption, intrusion prevention through application-level inspection, anomaly analysis and attack mitigation. Such devices need to have links to supporting systems. Much of this is already available, such as AAA, NAC links to virus and OS via CTA, NBAR links to PDLM modules for application recognition, but more is required, especially if the network is to have the ability to absorb attacks instead of just blocking them.

True network security intelligence will be a network that can automatically gather information on known attacks from various sources, monitor the data that it carries (on an infrastructure scale, not per element), analyze that traffic for known and also potential attacks (using anomaly detections), reconfigure itself to control the attack and report what is happening.

This will be a true, Self-Defending Network.

References

[1] Cisco Systems Inc. Charles Waltner "Cisco CEO Chambers Details Company's Vision for Network Security" Feb 22 2005 http://newsroom.cisco.com/dlls/2005/ts_022205.html

[2] Cisco Systems Inc. "Network Security Features on the Cisco Integrated Services Routers" 2005
http://www.cisco.com/en/US/products/ps5854/products_data_sheet0900aecd80169b0a.html

[3] Cisco Systems Inc "Network Admission Control – Current Participants"
http://www.cisco.com/en/US/partners/pr46/nac/partners.html

[4] Cisco Systems Inc "Network-Based Application Recognition IOS 12.2T"
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cd0.html

[5] National Security Agency "Router Security Configuration Guide" Dec 2003
http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf

[6] Internet Engineering Task Force - Rekhter/Moskowitz/Karrenberg/de Groot/Lear "RFC 1918 – Address Allocation for Private Internets" Feb 1996
http://www.ietf.org/rfc/rfc1918.txt?number=1918

[7] Internet Assigned Numbers Authority "Internet Protocol V4 Address Space" Jan 2005
http://www.iana.org/assignments/ipv4-address-space

[8] Internet Engineering Task Force - Ferguson/Senie "RFC 2827 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" May 2000
http://www.ietf.org/rfc/rfc2827.txt?number=2827

[9] Cisco Systems Inc. "Cisco Powered Network Program – Eligibility and Requirements"
http://www.cisco.com/en/US/applicat/cpnapply/applications_user_agreement.html

[10] Cisco Systems Inc. "Cisco Security & VPN Certification/Evaluation"
http://www.cisco.com/go/securitycert

[11] ICSA Labs "4.x Certified Firewall Products" Oct 2004
http://www.icsalabs.com/html/communities/firewalls/newsite/cert2.shtml

[12] Internet Engineering Task Force Killalea "RFC 3013 – Recommended Internet Service Provider Security Services and Procedures" Nov 2000
http://www.ietf.org/rfc/rfc3013.txt?number=3013