

White Paper

DEFENSE IN DEPTH

A Strategy to Secure Federal Networks

Juan Paul Pereira
Sr. Technical Marketing Manager



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200062-001

Contents

Introduction.....	3
Challenges of the U.S. Government in Information Security.....	3
Defense in Depth Strategy for Information Security	3
Principles of Defense in Depth.....	5
<i>Principle 1.</i> Deploy security solutions everywhere.....	5
<i>Principle 2.</i> Use multiple layers of security solutions to protect the network against intrusions and attacks	5
<i>Principle 3.</i> Protect the support infrastructure.....	5
<i>Principle 4.</i> Collect and analyze security events to determine threat levels.....	5
Benefits of Defense in Depth	6
Defense in Depth: The Nimda Worm Example.....	6
A Defense in Depth Framework Developed by the U.S. Department of Defense	7
Juniper Networks Solution for Defense in Depth.....	9
Conclusion	10

Introduction

U.S. federal agencies depend on their computer network infrastructure to perform critical functions; as a result, successful attacks on government networks can have major consequences on the nation. This paper describes Defense in Depth, a strategy being used by U.S. federal agencies to protect their network infrastructures. This paper also describes how Juniper Networks security solutions can be deployed to support a Defense in Depth strategy.

Challenges of the U.S. Government in Information Security

In the United States, the information revolution has changed the way government agencies operate. The U.S. government has moved critical processes to networked computers, and this trend to utilize computer networks continues. The migration towards widespread use of computer networks can expose security flaws, leading to attacks on government networks that could have serious consequences to the nation, such as disrupting critical operations, loss of sensitive information, or even loss of life.

The Government Information Security Reform Act (GISRA) requires that federal agencies conduct annual IT security reviews of programs and systems with the results of those reviews reported to the Office of Management and Budget (OMB) and the Congress. The reviews in recent years have identified numerous IT security weaknesses in federal networks. While some agencies have shown progress, significant challenges still remain in most federal agencies to secure their networks and systems. To improve the security of the government IT infrastructure, the current administration has directed significant resources to IT security (\$4.2 billion in FY03 and a requested \$4.7 billion in FY04).

In addition to improving the security of the IT infrastructure, federal agencies have also been directed to efficiently use IT resources and budgets. The U.S. federal government uses certain guidelines to improve their use of resources, including

- Sharing network and security infrastructure among government organizations
- Using commercial-off-the-shelf (COTS) security solutions to protect the government infrastructure
- Constantly monitoring the effectiveness of security programs

With the objective of improving the security of the infrastructure and the effectiveness in the use of resources, federal organizations are adopting Defense in Depth strategies, which allow them to map security needs with cost-effective security architectures and solutions.

Defense in Depth Strategy for Information Security

Defense in Depth is a term commonly used by the military to describe security measures that reinforce one another, hiding the defense mechanisms from view of adversaries, and

allowing the defender time to respond to attacks. In information security, Defense in Depth is used to describe a layered security approach. A Defense in Depth strategy uses several forms of network security mechanisms against an intruder and does not rely on one single defensive mechanism to protect systems or resources. By implementing multiple layers of security, a hole or flaw in one layer is covered by the other layers. An attacker will have to break through each layer without being detected in the process.

Faced with increasingly sophisticated attacks and expanding networks, network administrators realize that a single point or layer of defense, no matter how robust, can leave the network exposed. Defense in Depth establishes multiple layers of defense, all working in parallel. A simple example of a Defense in Depth strategy is illustrated in Figure 1. This network uses firewalls at the outer and inner network boundaries, with the inner firewall implementing more granular access control and user authentication. A potential attacker has to break through both firewalls to successfully compromise internal networks and systems.

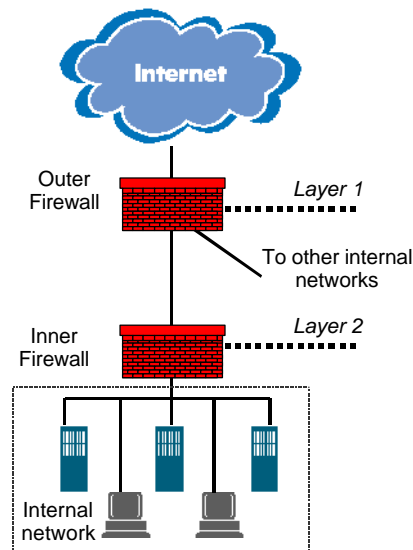


Figure 1. Example of a Defense in Depth strategy using two firewalls to provide multiple layers of protection. The inner firewall provides more granular access control and user authentication.

Defense in Depth involves using not only multiple layers of security but also complementary technologies at each layer. For instance, network administrators may deploy firewalls, intrusion detection and prevention, virus scanners, and content filtering at the perimeter to protect against external attacks and in the internal network to protect against internal attacks. Each technology and each layer complement the protection provided by the other security technologies and layers.

Most organizations acknowledge that intrusions and attacks are inevitable; a Defense in Depth strategy makes their success significantly more difficult. While attackers are breaking through defenses, network administrators have time to react to intrusions and are able change the security posture of the network infrastructure to prevent further damage.

Principles of Defense in Depth

The IATF defines four basic guiding principles¹ for Defense in Depth. It is important to observe that Defense in Depth does not dictate any particular security design; however, it uses certain guidelines that must be taken into consideration during the design and deployment of a network security infrastructure.

Principle 1. Deploy security solutions everywhere

Defense in Depth involves the deployment of protection mechanisms at multiple locations to resist all classes of attacks. When the network infrastructure is distributed, it is important to have proper security mechanisms at different areas to protect all networks from attacks.

Principle 2. Use multiple layers of security solutions to protect the network against intrusions and attacks

Defense in Depth includes deploying multiple layers of defense between the adversary and his target. Multiple defenses include firewalls, intrusion detection and prevention, virus scanning, and other technologies, all working in parallel. Figure 2 briefly describes a set of technologies available to implement each layer of defense.

Technology	Description
Firewall	Enforces access control on network traffic, selectively allowing external entities to access information protected by it. Firewalls are also used for denial-of-service (DoS) protection to defend networks against external or internal DoS attacks
VPN	Provides confidentiality and integrity to the data transmitted across a public network. VPNs also facilitate the implementation of communities of interest (COIs)
Intrusion Detection and Prevention (IDP)	Detects and blocks network attacks. IDP systems use knowledge of higher level protocols and applications to identify network attacks
Content Filtering	Performs content checking mechanisms for passing data, including anti-virus detection and protection
Public Key Infrastructure (PKI)	Authenticates users, devices and applications when sending, receiving or accessing information

Figure 2. Example of security technologies to implement a Defense in Depth architecture

Principle 3. Protect the support infrastructure

Networks, systems and security mechanisms depend on a support infrastructure, which must be protected from adversaries. The support infrastructure includes elements such as Public Key Infrastructure (PKI), directory services, and user authentication infrastructure.

Principle 4. Collect and analyze security events to determine threat levels

Defense in Depth includes the continuous collection and analysis of intrusions and other

¹ IATF – Information Assurance Technical Framework, Release 3.1, 2002, <http://www.iatf.net>

security events. This information is used to determine the threat levels of network infrastructure, so that network administrators can properly and promptly react to changes in the threat levels and adjust the security posture of the network, if required.

When implementing Defense in Depth strategies, federal agencies should consider these principles, so that security is properly implemented across the entire network infrastructure. In particular, federal organizations should define security architectures that rely on COTS security solutions and that achieve high levels of protection, assurance, and reliability at an acceptable cost.

Benefits of Defense in Depth

Defense in Depth strategies for information security offer significant benefits to federal agencies, including:

- Making it harder for intruders to penetrate all defenses to compromise the security of the network
- Greatly reducing the likelihood of a complete security breach
- Minimizing the time required for network administrators to detect and react to intrusions and attacks
- Accelerating the deployment of modular security architectures that can be implemented in phases
- Lowering budgetary expenditures by allowing federal agencies to utilize commercial-off-the-self (COTS) security solutions

In brief, Defense in Depth allows federal agencies to improve the security of their networks by deploying a cost-effective security infrastructure that is modular and uses COTS solutions. U.S. government networks cannot reach the point of total security; however, by using a Defense in Depth strategy to build multiple security layers, they can obtain the highest levels of network protection with reasonable investments.

Defense in Depth: The Nimda Worm Example

The Nimda worm hit the Internet in 2001, attacking networks worldwide and causing major problems to organizations. Government organizations were not immune to the effects of the Nimda worm. Specifically targeting Microsoft Windows computers, Nimda used multiple attack methods including: Microsoft IIS and Internet Explorer exploits, and email and Windows file-sharing propagations. As part of a Defense in Depth strategy, organizations could have used some preventive and reactive mechanisms to avoid the attack completely or to minimize its impact, including:

- Ensuring that critical servers were up to the latest patches and fixes
- Segregating public servers from internal servers
- Enabling private virtual LANs (VLANs) in DMZs to prevent compromised public servers from affecting other systems

- Enforcing access policies that restrict the connections from public servers to internal systems, unless required by the application
- Implementing security solutions to protect internal networks
 - Infrastructure firewalls to monitor internal traffic
 - Anti-virus software with updated virus signatures
 - Regular audits to discover vulnerable hosts
- Using response teams to quickly identify the worm and isolate the infected networks through internal network segmentation

Each of these mechanisms could be part of a Defense in Depth strategy. In this example, no single mechanism would have eliminated the attack, but two or more mechanisms would have minimized its effects. Federal defense agencies that had implemented some of these mechanisms significantly lessened the effects of the Nimda worm, and even when some servers were compromised, the worm did not affect other elements of their network.

A Defense in Depth Framework Developed by the U.S. Department of Defense

Defense in Depth is widely used in the U.S. Department of Defense (DoD). In this paper, we use a framework developed by the U.S. Department of Defense² to describe additional elements that can be used when implementing Defense in Depth strategies.

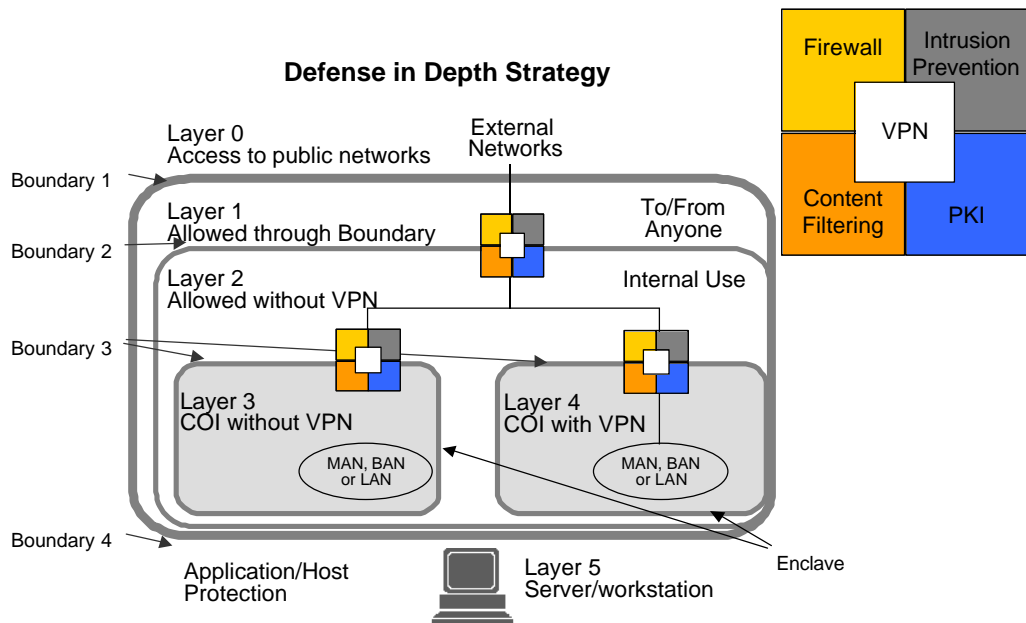


Figure 3. Example of a Defense in Depth security framework used by the U.S. Department of Defense, which illustrates various network boundaries used to protect end systems against attacks and intrusions

² NMCI Active Computer Network Defense Strategy, Department of Navy (DON), May 2002

The framework illustrated in Figure 3 uses multiple network boundaries that demarcate multiple layers of security. Each network boundary implements a set of security technologies that protects other layers from potential attacks. For example, defensive mechanisms at Boundary 1 may include firewalls and intrusion detection and prevention systems to inspect traffic coming from external networks. As traffic crosses network boundaries, it moves between security layers. In this particular framework, external traffic must cross four network boundaries (the last boundary implemented at the host-level) before it can reach end systems. The number of network boundaries protecting each asset depends on the criticality and security requirements of the asset.

Implementing multiple network boundaries allows for broad protection policies at outer boundaries and more granular security policies closer to the end systems. For instance, networks may require strong user authentication at the entry point of a sensitive network subnet (i.e., LAN), which can be implemented by firewalls and/or Virtual Private Networks (VPNs) at Boundary 3.

Figure 3 also illustrates enclaves, which are computing environments under the control of a single authority with personnel and physical measures, and under a single security policy. A single enclave includes local area networks (LANs), network resources, application and communication servers, and local switching and routing equipment. Enclaves may span a number of geographically separate locations with connectivity via a private network, and a single physical facility may have more than one enclave present.

By establishing network boundaries, network administrators are able to change the security posture of an enclave and effectively isolate enclaves from the rest of network infrastructure when threat conditions change. For instance, when the threat level increases, indicating that the network infrastructure is at higher risk, a military command may decide to isolate itself from the rest of the network but maintain communication within the enclave. Boundary technologies, including firewalls and VPNs, are used to change security postures and isolate network segments³.

DoD's Defense in Depth framework also uses Communities of Interest (COIs) to protect the communication of private communities. COIs generally involve geographically dispersed users or applications that exchange private information and require tighter security. By establishing COIs, organizations are able to compartmentalize networks yet provide common security services to all users of the network infrastructure. The DoD security framework in Figure 3 uses two types of COIs, COIs with VPNs, which interconnect elements via virtual private networks, and COIs without VPN, which interconnect elements using the public communication infrastructure.

³ See Juniper Networks CESAC white paper for more information about Security Management in federal networks

Virtual private networks facilitate the use of public communication infrastructure, encrypting the communication as it traverses the public infrastructure and excluding entities outside a defined COI. The desired result of establishing COIs with VPNs is to connect a larger community in a manner that provides unimpeded communication between the members, denies access to the information by any outside the community, and provides privacy of the information.

The concepts of this security framework, including network boundaries, security layers, enclaves, and communities of interest, can all be part of security architectures for federal government networks. The complexity of the architecture and the number of network boundaries will depend on the size of the network and the security requirements of the information being protected.

When using Defense in Depth strategies, federal agencies need to define security architectures that clearly demarcate security layers and network boundaries. The architecture should also identify the requirements for each network boundary and then map specific security solutions to meet these requirements. The Defense in Depth security architecture should use readily available technologies and be designed to offer the protection, assurance, and reliability required by the federal agency.

Juniper Networks Solution for Defense in Depth

Juniper Networks security solutions are being used to support Defense in Depth strategies in federal agencies. Juniper Networks integrated firewall and VPN product line provides firewall protection and VPN capability to be used at any network boundary. In addition, Juniper Networks firewall and VPN product line integrates with third-party technologies to offer a comprehensive solution for content filtering, including virus scanning and URL filtering. The Juniper Networks IDP product line offers intrusion detection and intrusion prevention functionality to detect and protect against application-level attacks by performing application-level inspection of the traffic.

Juniper Networks broad product line of firewall, VPN and intrusion detection and prevention solutions cover the security and performance requirements of any network size, allowing federal agencies to deploy security everywhere in the network, from remote sites with low throughput requirements to central sites with multi-gigabit demands. In brief, Juniper Networks line of security solutions implements many technologies and many layers of a Defense in Depth security architecture.

Juniper Networks firewall and VPN solutions are based on high-performance purpose-built security appliances that offer predictability under load and complete reliability. In addition, Juniper Networks firewall and VPN solutions incorporate denial-of-service (DoS) protection, permitting networks to offer continuous and reliable service, even under network attacks. Juniper Networks firewall and VPN solutions have received FIPS and Common Criteria certifications and can be freely used by U.S. civilian and defense agencies.

Juniper Networks firewall and VPN solutions also support the implementation of communities of interest (COIs). Unlike VPN only solutions that do not restrict the type of information carried through the VPN, Juniper Networks integrated firewall and VPN solutions allow federal agencies to implement network access control in addition to VPN encryption. Juniper Networks built-in firewall offers security to the peers connecting at each side of the VPN, so that they can enforce security policies for the communication.

Juniper Networks security management system allows network administrators to centrally monitor and control the security policies of the network. When threat levels change, Juniper Networks centralized management can easily change the security posture of the network to prevent further damage. Juniper Networks uses Command Enterprise Situational Awareness and Control (CESAC⁴) to deploy a security infrastructure and continually change the security posture of the infrastructure in accordance to threat conditions.

Juniper Networks is committed to providing high-performance, scalable and flexible security solutions to the U.S. government. Juniper Networks security solutions have been deployed by many defense and civilian agencies to implement multiple layers of Defense in Depth strategies.

Conclusion

Defense in Depth describes a multi-layer security architecture that combines security mechanisms to form layers of protection that will reduce the risk of attacks or intrusions. With Defense in Depth, federal agencies can significantly improve their network security by deploying cost-effective solutions throughout the network infrastructure.

Juniper Networks provides security solutions to implement multiple layers of a Defense in Depth strategy, including integrated firewall/VPN solutions and Intrusion Detection and Prevention (IDP) solutions.

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

⁴ CESAC is an approach created by Juniper Networks to implement security management

Juniper Networks, Inc.
1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel