CAMPUS NETWORK

An Overview of Brocade and Network Security

BROCADE

CONTENT

INTRODUCTION 3

MANUFACTURING 4

PRODUCT PREPARATION 4

SECURITY-RELATED FEATURES 5

BROCADE SECURITY FEATURES 5

SECURITY AT THE NEXT LEVEL 7

INTRODUCTION

Cyber security is an escalating concern for every customer. With the constant threat of data leakage and both internal and external attacks, intellectual property theft is a critical issue for end users and the vendors who supply their infrastructures. The financial burden on enterprises is massive. According to the 2012 Cost of Cyber Crime study conducted by the Ponemon Institute, the average annual cost of cyber crime reached almost $9 million per company studied, and those costs are rising.

Successful attacks are on the increase. News of system vulnerabilities are quickly propagated through underground channels, and almost all operating systems are subject to malicious attack. Spending on malicious attack vectors is believed to be equivalent to the R&D budgets invested in developing new security systems. There are a lot of cracks in the security dam.

Defense in depth describes a layered approach to security in the IT world. As a networking solutions vendor, Brocade makes security a very high priority, applying a defense in depth approach from the time products are designed and built through their lifecycle in customer deployments.

Although Brocade uses many layers of defense in all its products, only five layers of defense in depth are discussed in this paper.

- **Layer 1:** Brocade builds and prepares hardware and software to prevent the introduction of embedded vulnerabilities.
- **Layer 2:** Brocade prepares products so that they are already in a secure state when delivered to customers, reducing the chances of an improperly configured device being put into production.
- **Layer 3:** Contains features built into products specifically for the purpose of securing the network.
- **Layer 4:** Contains the array of specialized products to enhance security.
- **Layer 5:** Contains the open product framework that ensures the largest available ecosystem of partner solutions possible, providing for a best-in-class solution tailored to any customer's specific needs.

> *"In my opinion, cybercrime is the greatest transfer of wealth in history....Symantec placed the cost of IP theft to the United States companies at $250 billion a year—global cybercrime at $114 billion annually ($388 billion when you factor in downtime)—and McAfee estimates that $1 trillion was spent globally under remediation. And that's our future disappearing in front of us. So, let me put this in context, if I could. We have this tremendous opportunity with the devices that we use. We're going mobile, but [our devices are] not secure. [They have] tremendous vulnerabilities. Our companies use these; our kids use these; we use these devices, and they're not secure."*
>
> –General K.B. Alexander, director of the National Security Agency (NSA) and chief at the Central Security Service (CSS)

MANUFACTURING

To guarantee the integrity of Brocade products, strict component sourcing is enforced. Brocade works through a qualified list of approved vendors and maintains control of Tier 1 components. Brocade operates through a tightly controlled material tracking process and regularly audits all suppliers to maintain component and raw material integrity.

All software builds are run through multiple virus scans throughout the development process and reside only on servers owned by Brocade. Automated malware scans guarantee a sterile development environment. Engineering code is released directly from Brocade to the factory via a secure network connection. Firmware and software installation are automated through a file source maintained by Brocade, and all installations are logged and validated.

PRODUCT PREPARATION

Many researchers estimate that 30 to 50 percent of security breaches are due to misconfiguration. Brocade Ethernet and Fibre Channel products ship with initial configurations that are the most appropriate and secure for each environment.

Brocade® NetIron® CES 2000, CER 2000, and XMR Series products ship in a Zero Trust state, making them more secure on their initial deployment. Since Ethernet networks can be accessed remotely as well as directly in the data center and across the campus, the Brocade NetIron Series products ship with each port in a “down” state. This means that administrators must manually configure port interfaces to activate them. By doing this, administrators are aware of precisely what access is allowed. Shipping in a fully permissive state, as some vendors do, is not only an open door to attack but puts a much larger burden on administrators to make sure the environment is secure.

Brocade campus network products are shipped with ports enabled, since they are typically not installed directly to a Wide-Area Network (WAN) interface that allows direct exposure to remote access. Since most data centers and campuses are physically secure, campus products are typically deployed in a more controlled manner.

Brocade ships Fibre Channel products with the management port and data ports enabled. Fibre Channel is not a Wide-Area protocol. Data access is available only to locally attached devices. Site security, therefore, should be restrictive enough to prevent rogue machines or devices from plugging into a port on the Fibre Channel fabric in the data center.

Zoning is the primary access control mechanism on the fabric. Zoning creates Device Connection Control (DCC) and Switch Connection Control (SCC) policies that determine which devices are allowed on the fabric and how the switches communicate with their peers. This limits the ability for someone to maliciously or accidently plug a rogue switch or device into another switch, granting it access to the Storage Area Network (SAN).

Switch-to-switch communication can optionally be encrypted using the AES256 standard. This functionality is built into every Gen 5 Fibre Channel port, allowing communications to take place at full line speed even when encrypted. Open ports can be disabled for an additional level of physical security, if desired. Brocade Fibre Channel products push current configurations and policies to authorized network elements when they join a fabric, reducing configuration time and limiting exposure to configuration errors.

For more information, see the following sections in the *Brocade Fabric OS Administrator’s Guide*:

- In-Flight Encryption and Compression
  www.brocade.com/downloads/documents/html_product_manuals/FOS_AG_710/wwhelp/wwhimpl/js/html/wwhelp.htm#href=encComp.20.2.html
- SCC Policies
  www.brocade.com/downloads/documents/html_product_manuals/FOS_AG_710/wwhelp/wwhimpl/js/html/wwhelp.htm#href=secPolicies.13.06.html
- DCC Policies
  www.brocade.com/downloads/documents/html_product_manuals/FOS_AG_710/wwhelp/wwhimpl/js/html/wwhelp.htm#href=secPolicies.13.05.html

SECURITY-RELATED FEATURES

All Brocade products provide Role-Based Access Control (RBAC), which allows customers to limit access to management and configuration functions internally and externally. This insures that only proper permissions are given to employees, contractors, and vendors, depending on which management roles they are assigned. Auditing is provided on all products, and secure management takes place over mechanisms such as Secure Shell (SSH). These functions are standard in the device operating systems.

By embedding sFlow technology into network router and switch Application-Specific Integrated Circuits (ASICs), Brocade delivers an "always-on" monitoring system that operates with wire-speed performance to measure vital network security statistics. Cost of implementation is dramatically lower as compared to traditional network monitoring solutions that use mirrored ports, probes, and line taps. Additionally, sFlow monitoring operates while imposing minimal resource impact.

For more information on sFlow for network traffic monitoring, see the *Brocade MLX Series and NetIron Family Configuration Guide*.
www.brocade.com/downloads/documents/html_product_manuals/NI_05400a_CFG/wwhelp/wwhimpl/js/html/wwhelp.htm#href=sflow.75.1.html

Maintaining current levels of software and firmware is a top priority for ensuring network security. To address these needs, Brocade provides two free network auditing and monitoring utilities. Brocade SAN Health provides a powerful SAN tool that gathers diagnostic information about the entire SAN, rather than manually tracking individual components. Brocade SAN Health provides a wide variety of useful features that make it easier to collect data, identify potential security, maintenance, and configuration issues, and audit these results over time. Brocade NET Health provides a similar functionality for Brocade Ethernet and IP products.

BROCADE SECURITY FEATURES

For specific security needs, Brocade builds specialized products designed to work with existing network infrastructures. These products include the Brocade ADX® family of switches, the Brocade Encryption Switch, wireless defense systems (AirDefense Enterprise Appliances for Brocade Mobility), telemetry solutions such as the Brocade MLX® and NetIron XMR Series Routers, and the Brocade Vyatta® family of virtual routers, which provide routing, firewall, and VPN services.

For more information, see:
Brocade Telemetry Solutions White Paper
www.brocade.com/solutions-technology/industry/federal/daa-big-data.page

The Brocade ADX Series provides inherent security capabilities of its own. It is designed to provide IPv4 to IPv6 translation functions and load balancing for servers, firewalls, and encryption key managers. The Brocade ADX switch has a feature that mitigates high-speed Denial of Service (DoS) attacks and TCP Synchronization (SYN) attacks. The Brocade ADX device will intercept any TCP SYN packet and respond on behalf of the target server. If the Acknowledgment (ACK) is properly received, the communication is allowed; if it is not, the connection is dropped. With the Brocade OpenScript® engine, customers can dictate access to sensitive data by designating allowed access via IP address. The Brocade OpenScript engine can handle both IPv4 and IPv6 traffic.

For more information, see:
Brocade ServerIron ADX NAT64 Configuration Guide
www.brocade.com/downloads/documents/html_product_manuals/SIADX_12500_NAT64/wwhelp/wwhimpl/common/html/wwhelp.htm#href=Layer6TO4.3.3.html#1157739&single=true

ServerIron ADX Security Guide
www.brocade.com/downloads/documents/html_product_manuals/SIADX_12500_SG/wwhelp/wwhimpl/js/html/wwhelp.htm#href=Securitytitle.1.1.html

The Brocade Encryption Switch is a foundational element of any security strategy. By encrypting data at rest, customers can create a Zero Target Environment (ZTE). A ZTE is the concept that data is at the core of any targeted attack. If the data can be properly encrypted, it basically hides or removes the target. Data classification strategies and Zero Target implementation should be core elements in any security plan.

The Brocade Encryption Switch provides a storage security service in the data center fabric. An encryption device can encrypt data between any two ports in the Fibre Channel fabric. End devices do not need to be directly attached to the encryption devices to use the resource. Depending on the bandwidth requirements of the applications and how many encryption devices are deployed, the encryption resource can service tens or even hundreds of servers and storage devices. Each encryption device provides 96 gigabits-per-second (Gbps) of encryption bandwidth. Brocade encryption devices can be deployed as a highly-available, fabric-based product that interoperates with existing storage and servers.

For more information, see:
Encryption Solution Design and Deployment Considerations Best Practices
www.brocade.com/products/all/san-backbone-director-blades/product-details/FS8-18-encryption-blade/index.page

Wireless networks may be the most easily accessed component of the enterprise network. Because of this, Brocade wireless products provide many security-related features, including:

- Role-based wired/wireless firewall (Layers 2–7) with stateful inspection for wired and wireless traffic
- High-density active firewall sessions—205,000 per controller and 2,460,000 per cluster
- Protection against IP spoofing and Address Resolution Protocol (ARP) cache poisoning
- Per-user firewall options

Brocade also provides a wireless Intrusion Detection System and Intrusion Prevention System (IDS/IPS), including:

- Multimode rogue Access Point (AP) detection
- Rogue AP containment
- IEEE 802.11n rogue detection
- Ad-hoc network detection
- DoS protection against:
  - Wireless attacks
  - Client blacklisting
  - Excessive authentication/association
  - Excessive probes
  - Excessive disassociation/deauthentication
  - Excessive decryption errors
  - Excessive authentication failures
  - Excessive 802.11 replay
  - Excessive crypto IV failures (TKIP/CCMP replay)
  - Suspicious APs
  - Authorized devices in ad hoc mode
  - Unauthorized APs using authorized Service Set Identifier (SSID)
  - Extensible Authentication Protocol (EAP) flood
  - Fake AP flood
  - ID theft
  - Ad hoc advertising

The Brocade MLXe Series is the basis of a high-performance network telemetry-enabled security solution that can non-disruptively and transparently tap into a production network with no loss of performance. Brocade MLXe Series telemetry devices are able to replicate the ingress data to any number of egress ports by applying filtering rules while operating at full line rate. A sophisticated interface between the Brocade MLXe devices and analytic engines allow the filtering rules to be dynamically modified in real time based on the analytics that are performed. The Brocade MLXe devices can automatically load-balance intercepted traffic at a per-flow level towards individual—or clusters of—analytic engines. With industry-leading port densities, this provides a scalable, advanced, carrier-class security solution that focuses on the need for high-end, demanding customer environments where low-latency, throughput, flexibility, and performance are of paramount importance, yet constant security surveillance must be maintained.

For more information, see:
Brocade Security Analytics At-a-Glance
www.brocade.com/solutions-technology/industry/federal/daa-big-data.page

Now part of Brocade, the Brocade Vyatta family of products provides an application-centric approach to networking that delivers the industry's most comprehensive solution for complete migration of firewall, VPN, IPS, and dynamic routing to virtual environments. The Brocade Vyatta family ensures that organizations can segment, isolate, and secure data to meet the compliance requirements of next-generation virtual environments. Virtualization has changed the dynamics of security. The adoption of "Bring Your Own Device" (BYOD) and the heavy use of virtualization are altering the security space. The migration of data and workloads into the cloud or virtualized network space is forcing security administrators to rethink and possibly rearchitect their environments to provide the same level of data isolation and security controls that existed in their physical environments.

For more information, see www.vyatta.com.

Brocade has invested heavily in providing enterprises with security functions that extend from wireless to wired physical infrastructures, as well as to virtual and cloud infrastructures, ensuring the protection of customer data.

SECURITY AT THE NEXT LEVEL

Secure manufacturing, secure management and configuration, and RBAC are all basic elements of security implemented by Brocade products. Brocade has invested in core security competencies such as encryption of data, Distributed Denial of Service (DDoS) protection, and virtualized security—yet the threat landscape for network security changes daily. New exploits, zero-day threats, and advanced persistent threats create a continuous pressure on network security systems. It can be a huge challenge for an enterprise to keep ahead of rapidly evolving threats to security.

Brocade is implementing a strategy that allows our customers a "best of breed" approach. By partnering with the security companies with the highest expertise—those that continue to innovate against constantly changing threats—Brocade ensures that customers can cost-effectively integrate Security as a Service (SECaaS) into their corporate infrastructure. They can upgrade when needed and can leverage the best defense on the market at any given time, based on their specific security needs.

The Brocade strategy also allows customers to use a multivendor approach to infrastructure deployment, which typically means lower costs. To accomplish this interchangeable "best of breed" approach requires adherence to network standards and, in some cases, a unique implementation of technology—such as Brocade VCS Fabric technology. VCS Fabric technology:

- Offers support for the most demanding performance requirements
- Provides any-to-any communication
- Is Virtual Machine (VM)-aware
- Offers ease of use and operation

By leveraging an infrastructure based on VCS fabrics, customers have the ability to literally plug in security where necessary without rearchitecting the network and with minimal disruption. Customers can take advantage of the best-in-class offerings of IDS/IPS, firewalls, Network Access Control (NAC), and data analytics. The network can be built so that it is not only secure, but it can react to and identify threats in real time.

Brocade has tested and partnered with companies such as Palo Alto Networks, Symantec, McAfee, Impulse, IBM, Trend Micro, Check Point, FireEye, and many others to offer customers the ability to protect their data with the best offerings in the security industry, to ensure that their networks can adapt quickly to newly identified threats.

By providing an open standards compliant infrastructure, Brocade offers functionality such as load-balancing security appliances, to provide high-performance security monitoring at 100 gigabit Ethernet (GbE). Brocade can take alerts and disable ports on Brocade products based on flags from security vendors like McAfee and Palo Alto Networks. By being able to mirror flows at 100 GbE, Brocade can pass data traffic for real-time analysis and reaction. And, finally, by being able to encrypt data, Brocade can help the customer hide or remove the targets of attacks.

Defense in depth is a layered approach for securing critical environments and reaching necessary thresholds for compliance with regulatory standards such as HIPAA, PCI, and FISMA. By adopting the defense in depth approach, Brocade provides the blueprints for implementing secure solutions for critical data.

For more information, visit the Brocade Network Security page at:
www.brocade.com/networksecurity

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

BROCADE