

NATIONAL WATER QUALITY & AVAILABILITY MANAGEMENT (NAWQAM) SECURITY PROJECT:

After installation successfully the LAN and WAN; NAWQAM wants to implement a network security solution to protect this investment and avoid network down time because of hacking.

NAWQAM network Security will cover the two main sites at Shobra and Qanatir:

Solution Description:

Internet Router:

- Cisco Router 2610xm key features:
 - Performance is 20 Kpps
 - One Integrated 10/100 Mbps LAN ports
 - One Integrated Advanced Integration Modules (AIM) slots
 - Two Integrated WAN Interface Card (WIC) slots
 - One Network Module (NM) slot
 - 16MB Compact Flash and expandable to 48MB
 - 32MB DRAM and expandable to 128MB

Security Analysis:

Routers Are Targets:

Routers control access from every network to every network. They advertise networks and filter who can use them, and they are potentially a hacker's best friend. Router security is a critical element in any security deployment. By their nature, routers provide access and, therefore, you should secure them to reduce the likelihood that they can be directly compromised.

Switches Are Targets

Like routers, switches (both Layer 2 and Layer 3) have their own set of security considerations. Unlike routers, not as much public information is available about the security risks in switches and what can be done to mitigate those risks. Switches typically rely on virtual LANs (VLANs) for Layer 2 traffic segmentation.

Hosts Are Targets

The most likely target during an attack, the host presents some of the most difficult challenges from a security perspective.

There are numerous hardware platforms, operating systems, and applications, all of which have updates, patches, and fixes available at different times. Because hosts provide the application services to other hosts that request them, they are extremely visible within the network. For example, many people have visited www.whitehouse.gov, which is a host, but few have attempted to access s2-0.whitehouseisp.net, which is a router. Because of this visibility, hosts are the most frequently attacked devices in any network intrusion attempt.

Networks Are Targets

Network attacks are among the most difficult attacks to deal with because they typically take advantage of an intrinsic characteristic in the way your network operates. These attacks include *Address Resolution Protocol* (ARP) and *Media Access Control* (MAC)-based Layer 2 attacks, sniffers, and distributed *denial-of-service* (DDoS) attacks. Some of the ARP and MAC-based Layer 2 attacks can be mitigated through best practices on switches and routers. Sniffers are discussed in the primer at the end of this document. DDoS, however, is a unique attack that deserves special attention. The worst attack is the one that you cannot stop. When performed properly, DDoS is just such an attack. As outlined in Appendix B, "Network Security Primer," DDoS works by causing tens or hundreds of machines to simultaneously send spurious data to an IP address. The goal of such an attack is generally not to shut down a particular host, but rather to make the entire network unresponsive. For example, consider an organization with a DS1 (1.5 Mbps) connection to the Internet that provides e-commerce services to its Web site users. Such a site is very security conscious and has intrusion detection, firewalls, logging, and active monitoring. Unfortunately, none of these security devices helps when a hacker launches a successful DDoS attack. Consider 100 devices around the world, each with DSL (500 Kbps) connections to the Internet. If these systems are remotely told to flood the serial interface of the e-commerce organization's Internet router, they can easily flood the DS1 with erroneous data. Even if each host is able to generate only 100 Kbps of traffic (lab tests indicate that a stock PC can easily generate 50 Mbps with a popular DDoS tool), that amount is still almost ten times the amount of traffic that the e-commerce site can handle. As a result, legitimate Web requests are lost, and the site appears to be down for most users. The local firewall drops all the erroneous data, but by then the damage is done. The traffic has crossed the WAN connection and filled up the link.

Applications Are Targets

Applications are coded by human beings (mostly) and, as such, are subject to numerous errors. These errors can be benign—for example, an error that causes your document to print incorrectly—or malignant—for example, an error that makes the credit card numbers on your database server available via anonymous FTP. It is the malignant problems, as well as other more general security vulnerabilities, that need careful attention. Care needs to be taken to ensure that commercial and public domain applications are up-to-date with the latest security fixes. Public domain applications, as well as custom developed applications, also require code review to ensure that the applications are not introducing any security risks caused by poor programming. This programming can include scenarios such as how an application makes calls to other applications or the OS itself, the privilege level at which the application runs, the degree of trust that the application has for the surrounding systems, and finally, the method the application uses to transport data across the network. The following section discusses intrusion detection systems (IDSs) and how they can help mitigate some of the attacks launched against applications and other functions within the network.

Intrusion Detection Systems

Intrusion detection systems (IDSs) act like an alarm system in the physical world. When an IDS detects something that it considers an attack, it can either take corrective action itself or notify a management system for actions by the administrator.

Some systems are more or less equipped to respond and prevent such an attack. Host-based intrusion detection can work by intercepting OS and application calls on an individual host. It can also

operate by after-the-fact analysis of local log files. The former approach allows better attack prevention, whereas the latter approach dictates a more passive attack-response role.

Because of the specificity of their role, host-based IDS (HIDS) systems are often better at preventing specific attacks than network IDS (NIDS) systems, which usually issue only an alert upon discovery of an attack. However, that specificity causes a loss of perspective to the overall network. This is where NIDS excels. Cisco recommends a combination of the two systems-HIDS on critical hosts and NIDS looking over the whole network-for a complete intrusion detection system.

When an IDS is deployed, you must tune its implementation to increase its effectiveness and remove "false positives." False-positives are defined as alarms caused by legitimate traffic or activity. False negatives are attacks that the IDS system fails to see. When the IDS is tuned, you can configure it more specifically as to its threat-mitigation role. As mentioned above, you should configure HIDS to stop most valid threats at the host level because it is well prepared to determine that certain activity is, indeed, a threat.

Cisco PIX 515E Security Appliance

The Cisco PIX® 515E Security Appliance delivers enterprise-class security for small-to-medium business and enterprise networks, in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with DMZ support. Part of the world-leading Cisco PIX Security Appliance Series, the Cisco PIX 515E Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration capabilities, and powerful remote management capabilities in an easy-to-deploy, high-performance solution.

Cisco 4200 IDS Security Appliance

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Cisco Security Agents

The next-generation Cisco® Security Agent network security software provides threat protection for server and desktop computing systems, also known as endpoints. The Cisco Security Agent goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications.

Because the Cisco Security Agent analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs.

FORTINET TAKES REAL-TIME NETWORK PROTECTION TO THE EDGE

Threats to corporate networks have evolved beyond the capabilities of traditional, firewall-based defenses. Email messages, file transfers, Web-pages and VPN links are now used to introduce damaging viruses, worms and inappropriate content into data networks. Firewalls are powerless against most of these “content-based” threats — they simply weren’t designed to analyze and process the application-level contents of network traffic. Conventional, software-based solutions are complex, costly, and too slow for today’s real time communications.

At Fortinet, we went back to the drawing board and developed a new type of platform that can deal with today’s and tomorrow’s threats at the network edge, without slowing your critical network applications. We assembled a team of the world’s leading networking and security experts — including the creator of the world’s most successful network security appliance and one of the world’s most respected antivirus experts — and created the awardwinning FortiGate™ line of Antivirus Firewalls — the next generation in real-time network protection. The unique, ASIC-based architecture of Fortinet’s FortiGate platforms avoids the limitations of conventional firewalls, VPN gateways, and software-based antivirus and content filtering systems. They provide better protection, faster, and at lower cost.

FortiGate Antivirus Firewalls protect you against all of the key threats to your security and productivity, and offer an unmatched array of integrated, policybased capabilities. FortiGate units integrate seamlessly into your network, and can even provide antivirus and content filtering services “transparently” in conjunction with your existing firewall. FortiGate network protection systems have earned an unprecedented four certifications from ICSA for firewall, IPSec, antivirus, and intrusion detection.

Fujitsu offers an appropriate solution to match with NAWQAM environment; the following points briefing the solution:

- 1) At Shoubra, we will separate the Internet Connection to a Cisco 2610xm router, instead of connecting directly with the WAN HQ Cisco 3745 Router, with its security features (Firewall & Intrusion Detection System) for perimeter security.
- 2) Two Cisco PIX 515 Firewalls, Unrestricted Bundle, are already exist; so we will make use of them, one at Shobra site and the other one at Qanatir.
- 3) Additional optional PIX 515 Firewall Ethernet Card is offered to accommodate connecting the WAN sites to separate DMZ.
- 4) Additional optional PIX 515 Firewall Ethernet Card is offered to accommodate connecting the Web Sever or in the future any public servers to separate DMZ.
- 5) At Shoubra, Cisco Intrusion Detection Sensor 4235 will take place after the Cisco PIX firewall to monitor, detect, and respond to any hacking anomaly activities from the Internet and other WAN Sites.
- 6) Additional optional IDS 4-port Ethernet Card is offered to accommodate monitoring the Web Server DMZ.
- 7) At Qanatir, Cisco Intrusion Detection Sensor 4215 will take place after the Cisco PIX firewall to monitor, detect, and respond to any hacking anomaly activities from WAN Sites.
- 8) Cisco Security Agent (Host-Base IDS) will be installed on the mission-critical Servers to monitor and block any known or unknown anomaly behaviour at the seven servers.
- 9) Additional optional Cisco Security Agent is offered to cover the management workstation if needed.

- 10) We provide a Hardware-Based Antivirus, Firewall, IDS, VPN, and Content Filtering appliance (FortiGate-300) which provide back-to-back Firewall & IDS scenario providing an additional security layer.
 - 11) The FortiGate 300 also provide Antivirus Gateway at the Internet source; no virus from the Internet can infect any internal user at all NAWQAM Sites even if this user's machine does not have desktop antivirus or does not have the last virus definition updates.
 - 12) The FortiGate 300 also provide Content Filtering providing administrators the best usage from the Internet line by blocking all prohibited categorized websites.
 - 13) Security Management Software will monitor and manage all security equipment and configurations.
-