Communicating With Sam

Protecting the Network From the Inside Out

Sam Johnston

Question:

Our company is currently undergoing a merger with another company and I have the responsibility of securing and supporting our iSeries, Windows Server Farm, and the Desktop environment. Our company's data centre will stay the same but now we will need to support over 10 new remote offices and a dramatic increase in mobile workers.

With the acquisition our total number of office desktops will increase from 60 to over 300. Additionally, our mobile work force will increase from 20 users to approximately 80 users. How can I manage security during the transition and how can I ensure that all the devices accessing our datacenter are secure?

Response:

The challenge you face is significant. Some of the key concerns you have to manage are: qualifying who the user is (identity), what system they are accessing from (approved corporate PC, hotel or café desktop, family PC?), the state of standardization of the PC (anti-virus, Host Based Intrusion Detection Software, latest application patches, spyware, etc.), and origination of the connection (local office, remote office, VPN, WAN). Your ability to manage the security of your desktops just became more complex as geography, diversity of hosts and sheer volume of users has greatly added to your burden.

The solution to these issues requires the integration of security throughout the network, incorporating a collaborative process between network elements and security that will defend against known threats and adapt to new threats as they arise. In order to provide a comprehensive level of security, the network and security technology must focus on the following areas:

- **Secure Connectivity.** This ensures the privacy of information communicated across the network either internally or remotely.
- **Threat Defense:** Protection of Servers and Desktops from Worms, Viruses, Spyware, Denial of Service Attacks etc.
- **Trust and Identity:** Manage users and devices based on policy, providing approved access and use of applications.
- **Management:** Centralizing configuration of security devices and reporting of security events.

What if there was a solution that could be centrally managed that would assist in this task and automate much of the processes of managing the security of your network access while not requiring immediate standardization of the desktops and processes?

The solution you are looking for can be referred to as Network Admission Control. It is not a single device but is made up of layers of security that work together to provide a comprehensive solution to meet your needs. In this article we will focus on discussing Cisco's Network Admission Control via the Cisco NAC appliance, which has the benefit of rapid deployment and does not require standardization. Alternative solutions exist that support the NAC framework and that leverage technologies from multiple vendors and support some standards across the industry. Typically deploying these solutions is more complex than the Cisco NAC appliance and thus not likely your first choice, especially in a hybrid network environment brought on by your recent merger.

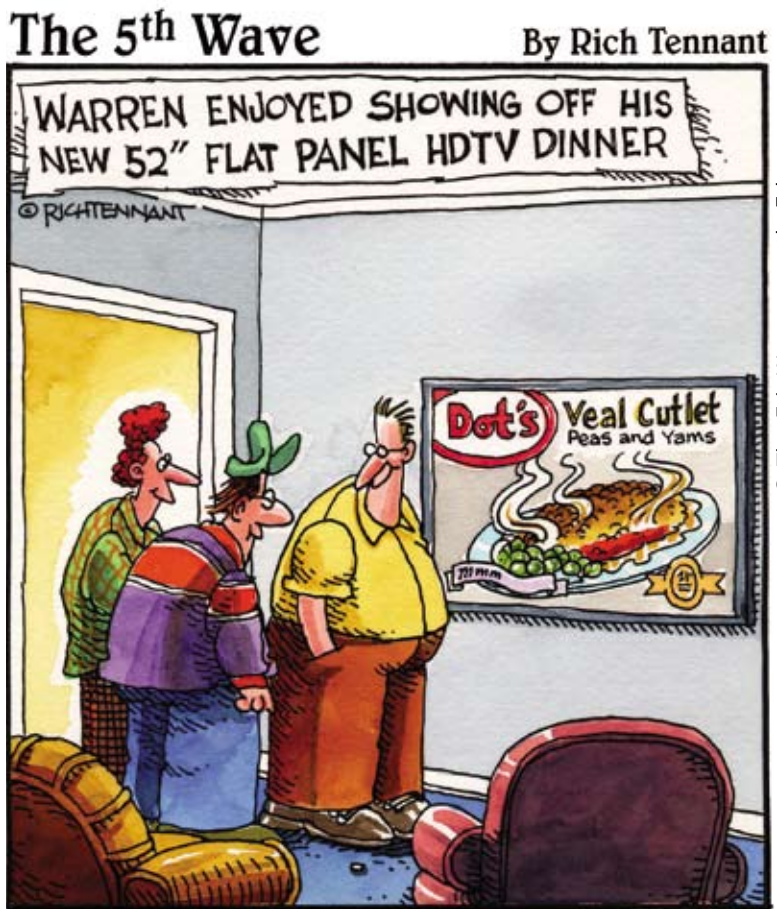
Let's discuss some of the standalone traditional systems used for security and management of network access. For the challenge of securing your remote access users there are many firewall/VPN solutions that can be deployed at the edge. These will provide a level of security in limiting what users connect and what hosts/network they can access. But what they cannot determine is if the host used to connect is compromised. Additionally, you may deploy technologies to the desktop such as anti-virus or HIDS but how can you know if they are operating at all times or whether the updates or policies are kept current. With a large organization performing this step manually can be very resource intensive. An additional consideration that is also overlooked is the LAN network. How can you efficiently ensure that all devices connected to your LAN ports are from trusted users and the devices are approved and properly provisioned systems?

This is where a comprehensive solution like Cisco's Network Admission Control Solution (NAC) can greatly assist in managing and mitigating these issues. The key architectural point in Cisco's solution is that it uses the network entry point as the point of enforcement of policies. The entry point can be configured as a standalone inline appliance for non-Cisco Switched deployments or the Cisco switched infrastructure can leveraged

where present to support an Out-of-Band centralized management mode. The four key NAC capabilities, as defined by Cisco, are (i) securely identify the device and user and link them together with policies, (ii) enforce consistent policy which makes end station security management more efficient, (iii) Quarantine and Remediate devices that are non compliant and have a centralized approach to fix defined gaps greatly reducing resource cycles within an organization, and (iv) enable ease of configuration and management of policies and groups.

At this point we will get into further detail of a key component in the Cisco NAC strategy, the Cisco NAC Appliance. The Cisco NAC Appliance solution components include; an optional Cisco Clean Access Agent that can be installed on client PCs to support registry scans of the client PC, a Cisco Clean Access Server, that can be installed in-band or out-of-band for Network Access Control, and a Cisco Clean Access Manager that is the centralized management point for the NAC solution. All these appliances can be provisioned in standalone or recommended failover model for high availability.

The Clean Access Server can be configured in-band or out-of-band in a centralized deployment. For in-band, all the user traffic must pass through the appliance so deployment must take this into account when defining where to place the Clean Access Servers. This deployment mode is usually best suited to non-standard switches. However, if you already have Cisco switches, than the appliance can be provisioned centrally and the switches can be configured to act as the control point for quarantine and leverage VLANs to isolate non-compliant users. There are a number of Out Of Band deployment modes, which provide flexibility for the different deployment requirements. Out-of-Band installations are preferred due to the increased reach of a single appliance and they eliminate choke points within the network created by an over worked inline device.



The Clean Access Server authenticates and authorizes users from a local db or can leverage a RADIUS, LDAP, Kerberos or AD database for access information. Based upon defined policies the Clean Access Server can scan PC for such things as virus infections, port vulnerabilities, OS load, antivirus or anti-spyware, operating services and files. For non-compliant devices the Clean Access Server can isolate the devices on a per-user level and assist in network based self-remediation. Remediation methods may vary by device and supported software and may be driven by CISCO NAC partner solutions such as Anti Virus update etc.

As you are aware the amount of workload of manually managing diverse access and many diverse hosts can be intimidating. A centralized management environment for device configuration, and security event reporting should be part of the corporate merger plans.

Implementing a Network Access Control solution using the Appliance model will allow you to quickly bring Trust, Identity and Threat Defense issues under control. The type of deployment method will be determined by the existing switch infrastructure. If your organization has standardized on a Cisco switching platform you will be able to leverage the intelligence built into it reducing the number of devices required and lowering the overall cost of the NAC solution. TUG

***Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday December 8, 2006.*

COiN Meeting Review — September 11, 2006

By Glenn Gundermann

COiN started off the season with veteran speaker **Richard Dolewski** presenting "Conducting a Best Practices Audit of your iSeries/400". We were enlightened as well as entertained over the course of two hours at Conestoga College in Kitchener.

Richard is a certified systems integration specialist and disaster recovery planner. If you attended the session, you would know why he is the winner of numerous speaking awards at COMMON and a member of the COMMON Speaker Hall of Fame.

Practical advice was given for often-neglected tasks. One good example of this was to secure your development environment. We take great lengths to secure our production environment and often make a complete copy into development but don't take the same precautions to secure this area. Another good example is to review default passwords. For those who didn't know, IBM's SECTOOLS menu is one valuable resource with many good options. One of them is the Analyze Default Passwords and another is to look for user profiles with a user class and special authority mismatch.

Don't forget to delete those user profiles for employees not there anymore, he says. Have you heard of "profile swaps"? If you are in charge of security, you had better take care of this. Another area to review is IFS security. We store more and more information on the IFS and the default authority is *PUBLIC(*ALL).

Auditing is not only a useful tool but also a must. As a **minimum**, you'll want to audit *SECURITY, *SAVRST, *AUTFAIL, *DELETE, *CREATE, and *SERVICE, plus everything QSECOFR and other *ALLOBJ users do. You should have exit points monitoring access for FTP, ODBC, etc.

Various best practices were covered including LPAR/HMC, backup & recovery, testing, plus others, with detailed points on each topic.

COiN speaker Richard Dolewski

"Boom is Bad!"

What I really enjoy from listening to Richard speak is his real-life experiences. We heard several stories including a customer in Mexico who finally agreed to going with a High Availability (HA) solution. This was his "Boom is Bad" story and demonstrated that different customers have different reasons for doing something. So whether you are located right beside another company that goes "Boom!" three times a year, or you want to eliminate your planned downtime from backups, it doesn't matter. Both are good reasons for HA.

Suffice it to say, it was a great session.

In summary, it's worth the drive to Kitchener to catch a COiN meeting! *

Richard Dolewski is VP of the Technical and Contingency services provided by Mid-Range, and can be reached at rdolewski@midrange.ca.

Eveline Gaede says, "Come on out for another great year of networking and learning!". COiN's next session on Nov. 6 is a two-part session on SOA. For more information, contact coininfo@coinusergroup.ca. TUG

Glenn Gundermann *is a TUG board member and chairs the TEC '007 committee. He can be reached at ggundermann@tug.ca.*

* Tug members are free to attend COiN meetings.