BearingPoint. Management & Technology Consultants

Best of the California, Security and Data Vulnerability Session

Securing Your Data, Infrastructure and Applications

Aaron Iacobucci
Director, Risk and Architecture Management – State and Local Government
aaron.iacobucci@bearingpoint.com, 512.542.3571

Remote Access Issues

Remote access to applications or systems:

Whether presented through the Internet or through other means, presents challenges that must be addressed within the applications and through infrastructure.

The following questions must be considered:

- How do you keep applications secure?
- How do you prevent brute forcing of accounts?
- How do you keep costs down?
- What operational issues will you face?
  - Patching
  - User Management
  - VPN Costs

Was the Application built for Internet or Intranet?

This question is important to consider because the way you allow personnel to access the application would be different for Internet verses Intranet applications.

Also the sensitivity of the data may determine how you deploy the application.

If the application was built properly for the Internet, it will have a certain amount of security features built into it:

- Login a limits such as lockout features after multiple attempts
- Input validation to prevent various type of application level vulnerabilities (SQL Inject, buffer overflows, etc.). See www.owasp.org for a good source of application coding standards.
- Session state management to prevent viewing sensitive information or jumping from account to account.

Was the Application built for Internet or Intranet?

If the application was built properly for an Intranet, it will be built based upon a certain amount of trust implied within an organization.

- User credentials may not have detailed requirements and may allow weak passwords with no lockout features.
- Authentication may just be pass-through from LDAP or Active Directory
- There may be little or no validation on input fields.
- The web and application logic are not separated and database access may be directly from the web layer.

However, remember that even on Intranets, you have risks…

Access for Internet Applications

Access for Internet based applications is fairly straight forward.

- Deploy the application in a secure environment.
- Provide appropriate firewall and monitoring.
- Configure the application.
- Allow access.

Internet applications usually have mechanisms that prevent brute forcing accounts if the data is sensitive

Access for Intranet Applications

Intranet applications are almost never allowed access directly through from the Internet.

These application typically provide day-to-day functions for the business and many times contain sensitive data. Having the application disrupted or the information stolen or corrupted could be disastrous for the company involved.

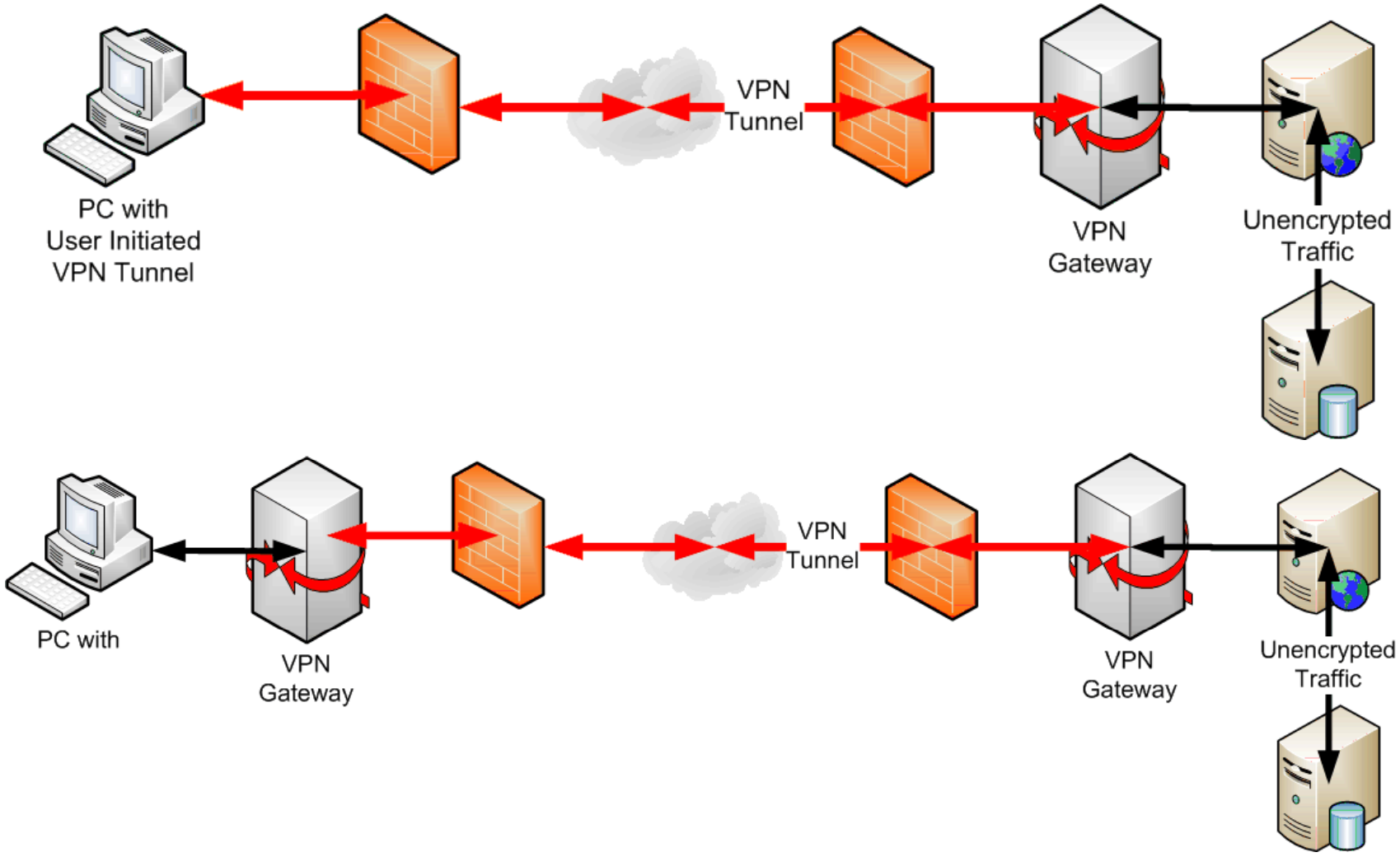
These applications are typically deployed on an internal network that is available to employees connected to the company network and remote access is through a VPN or through some sort of advanced authentication such as certificate authentication or two-factor authentication.

Virtual Private Network Basics

Virtual Private Networks (VPNs) provide a method of connecting to a remote site through an “encrypted tunnel”. In short, it means that all the communications between the two points are encrypted.

- VPN tunnels can be initiated by end users when needed
- Can be setup system to system
  - Used when communications between systems is very sensitive.
  - IPSEC is often used as a VPN tunnel between systems
- Can be setup site to site
  - Used when there is a significant amount of traffic between two sites or the connection must be available all of the time.
- VPNs usually have mechanisms to prevent brute forcing accounts

Virtual Private Networks
User-Initiated versus Lan-to-Lan



Types of Authentication

Simple Username and Password

Username, Password, and VPN Certificate

- Many VPNs require a group certificate in order to connect
- Certificate is issued by security or network group and is the same for everyone in the VPN group

Two-Factor Authentication

- Something you know and something you have
  - Could be a certificate installed on your computer that is specific for your computer or you
  - One time use passwords
  - Tokens
- Unique for every person
- Provides validation that you are who you say you are

Operational Issues

- VPNs must be maintained and takes advanced skills to set them up.
- These systems must be patched like any other system
- Maintenance costs are typically 27% of operational costs of these systems
- Two-Factor authentication is more expensive.
  - Costs of tokens for each person
  - Costs of licenses for each person
  - If certificate servers are used, must maintain good backups of certificate server
    - Loss of certificate server means all certificates must be rebuilt and reissued
  - Operation costs of maintaining users and other administrator costs and distributing certificates or tokens

Limiting Costs

Use ‘Quality’ Internet programs where available

Consider SSL VPNs

Use Two-Factor authentication only for sensitive tasks or accessing sensitive data

Hire knowledgeable personnel and plan you work carefully.

- The cost of a breach or having to rework later is more costly than hiring someone who knows what they are doing
- Hire a contractor that specialized in this area if you can’t afford full time personnel.

Check out these websites

- www.pcisecuritystandards.org
- www.bearingpoint.com/securityingovernment
- www.owasp.org

Come visit at booth 24

Panel Questions