

Weekly Q&A with Moose Logic



Audio Announcement: Select your audio now. To dial the conference, select “Use Telephone” in your audio pane and enter your unique audio PIN. By default, you have joined audio using your computer’s speaker and microphone system (VoIP).

Submit Your Questions: Select “Questions” to type your question(s). Your question will be read to the audience and addressed during the Q&A section of this webinar.

Weekly Q&A with Moose Logic

Secure Remote Access with SSL

Presented by Garry Corbin
October 20, 2010

Agenda

- Introduction: 5 - 10 minutes
 - What is driving the need for SSL VPNs?
 - Business Impact of Traditional Access
 - Common Use Cases
 - Introducing WatchGuard SSL
 - Benefits Summary
- Q&A: 15 - 20 minutes
 - Submit your typed questions within the Questions section.
 - Questions requiring more research will be answered by email AND within the attachment to this webinar's archive



What is driving the need for SSL VPNs?

Globally distributed network

Need to do more with fewer resources

- Anytime, anywhere access from virtually any device
- Per user resource and application access

Consequences of non-compliance

- Failed audits (PCI-DSS, SOX, HIPAA)
- Remote vulnerabilities
- Out-dated technologies

Explosive growth in network size and technologies

- Increasing mobile & partner work force
- New services and applications
- More and more platforms

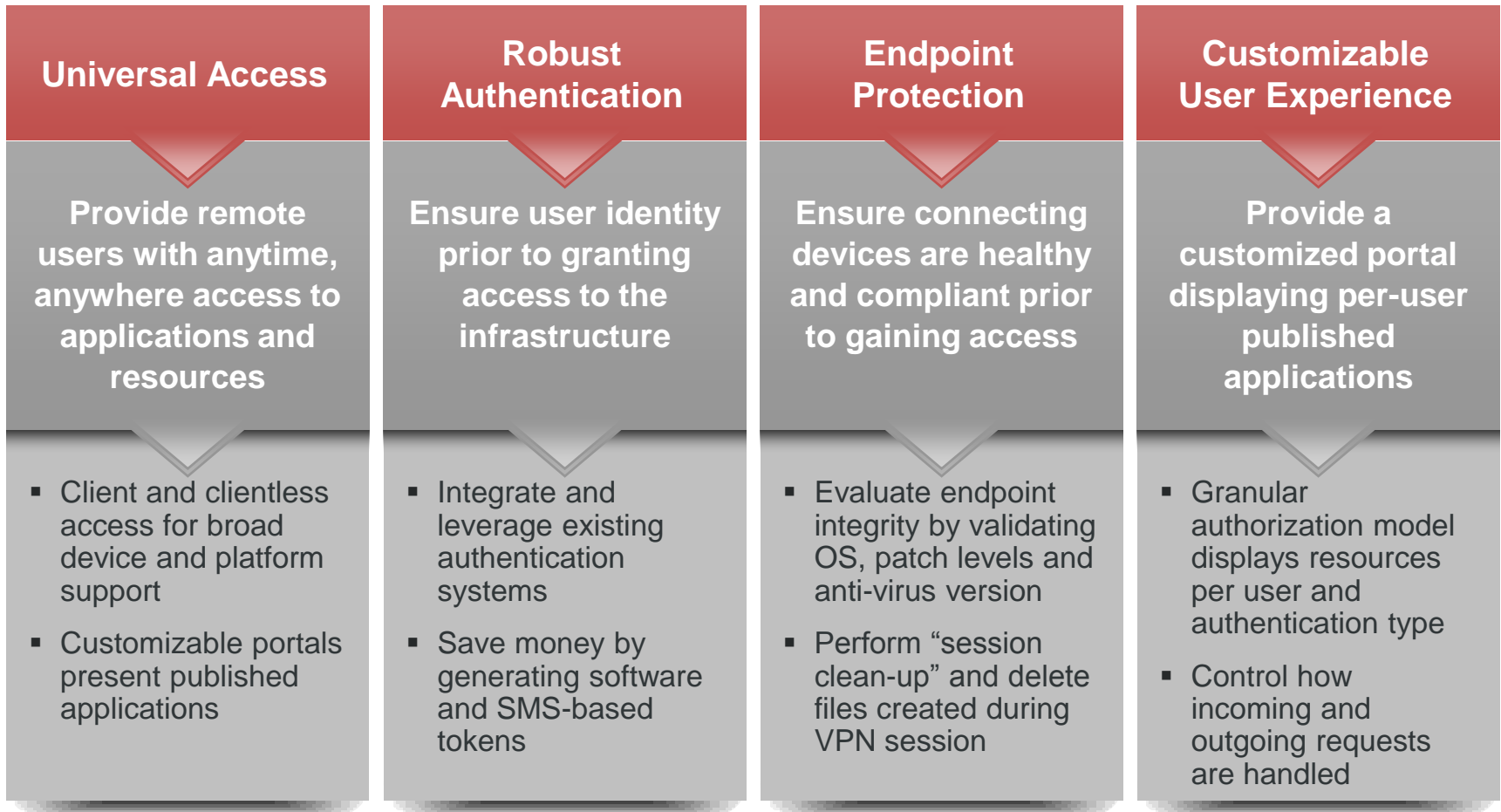
Rising operational costs

- Lack of visibility and reporting
- Client software support costs

Business Impact of Traditional Access

Costly deployments	Requiring client software limits device support and increases deployment costs
Risk to internal network resources	Unhealthy remote devices can open windows of vulnerability and introduce malware to networks when connecting
Complex, labor-intensive ongoing support	Client software version management, unhealthy remote devices and firewall issues increase management overhead
Growing compliance requirements	Regulatory requirements demand more granular access and authorization controls along with the ability to audit and report

Common Use Cases



Introducing WatchGuard SSL

- WatchGuard SSL 100 and SSL 560
 - For small-to-medium enterprise organizations
 - Highly secure remote connectivity for a myriad of mobile devices and platforms
 - Delivers business applications to the user for maximum productivity
 - Most comprehensive array of authentication, identity management and security features
 - Web browsers or thin clients
 - Endpoint integrity checking
 - Network interface control
 - Virtual desktops
 - Session clean-up



Benefits Summary

Increased productivity	Deliver critical applications to users' desktops – anytime, anywhere and on virtually any device
Lower ownership costs	Less to manage – no clients, stronger security and an easy-to-use centralized administration server
Compliance assurance	Set granular access policies that match requirements, as well as audit and generate reports for compliance due diligence
Resource scalability and availability	Achieve 100% planned network uptime and scale the size of a deployment to the number of users in an organization
Build security awareness	LiveSecurity Services provide technical support and up-to-the-minute security analyses, articles and podcasts

Q&A



- Additional resources
 - One-on-one whiteboard discussions***
 - sales@mooselogic.com
 - 206-774-0619 Ext. 102
 - Online***
 - www.mooselogic.com/blog
 - www.watchguard.com/SSL
 - wwwwatchguard.com/education
- Future webinars
 - www.mooselogic.com/events

Use Case: Universal Access

The challenge

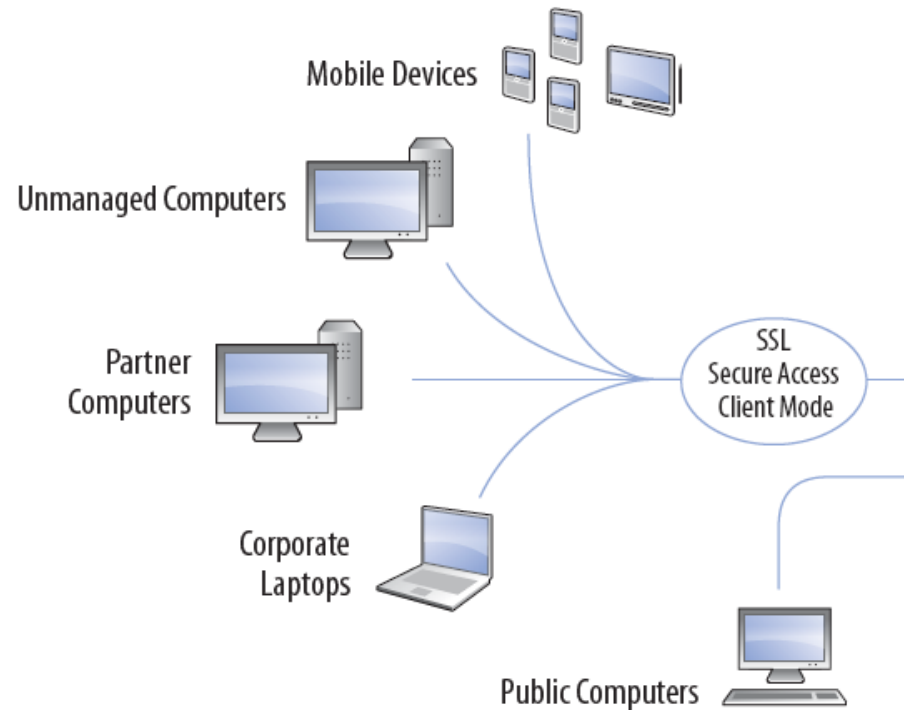
Organizations want to deliver critical business applications to the desktops of remote users and partners anywhere, anytime to maximize productivity

WatchGuard solution

Browser or thin client provides broadest device access

Support for generic tunnels and “kiosk mode” equals greater access to applications and resources

Broad Platform and Device Support



Use Case: Robust Authentication

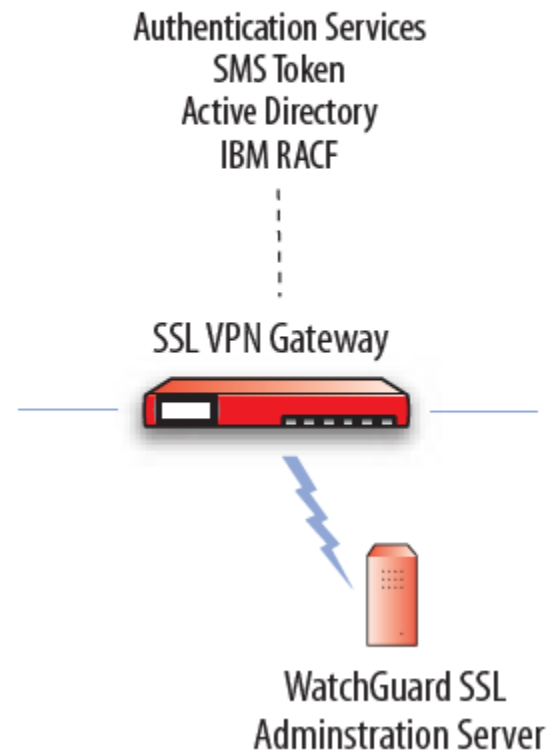
The challenge

Organizations want to ensure two-factor authentication for remote VPN users without increasing costs

WatchGuard solution

Allows organizations to use integrated software or SMS-based token functionality with WatchGuard SSL to validate user identity with a computer or mobile phone at no additional cost

Comprehensive List of Authentication Types



Use Case: Endpoint Protection

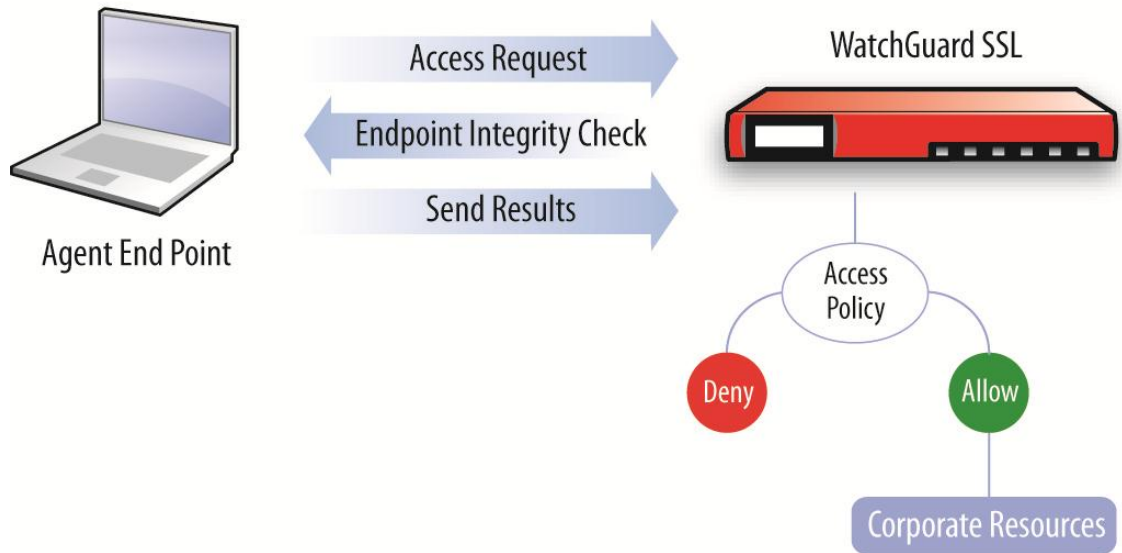
The challenge

Organizations want to maintain the uptime of remotely accessed resources and ensure mobile and remote users do not introduce malware to production systems

WatchGuard solution

WatchGuard SSL performs pre-connection endpoint integrity checking to ensure remote device are healthy and policy compliant. Devices are cleaned of temporary files at the end of their VPN session

End Point Integrity Checking



Use Case: Customizable User Experience

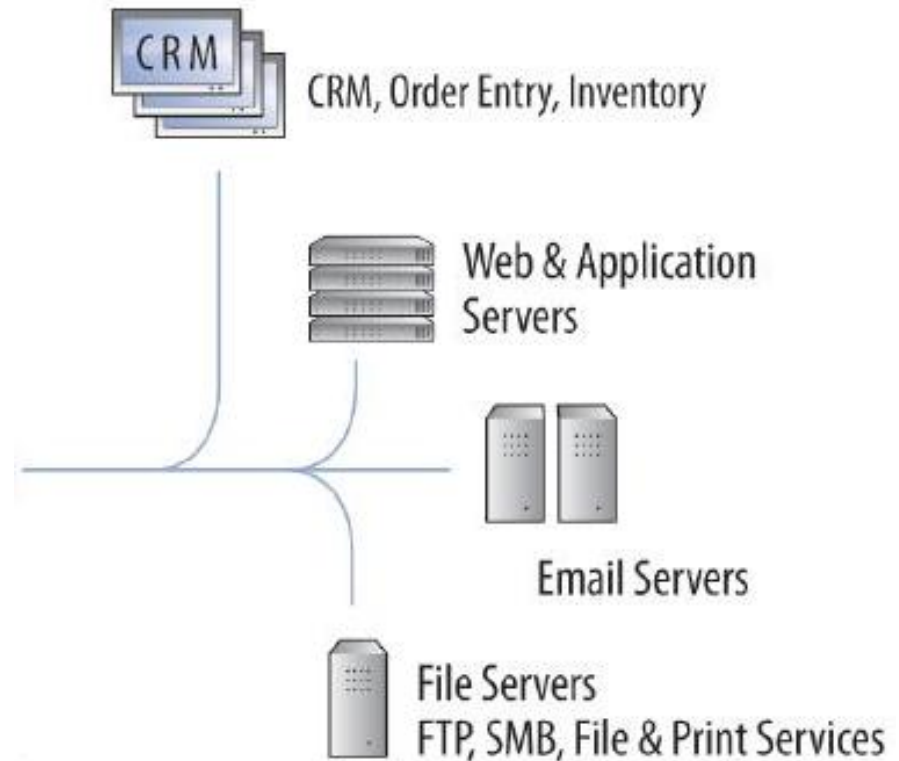
The challenge

Organizations want to provide users with a custom-tailored experience that delivers only the applications and resources for which the user is authorized

WatchGuard solution

WatchGuard SSL possesses an extensible authorization model and presentation layer allowing organizations to customize the look and feel of each user's portal, as well as control how the user routes network requests

Wide Access to Corporate Resources



Deployment Architecture

WatchGuard SSL Deployment

