



## Secure Network Connections For Vector Vision Hosted Services

A hallmark of Consistacom's Vector Vision Hosted Service delivery is the use of secure data exchange between Consistacom and your Avaya telephone system. This is the fastest, most secure, and most cost-effective way to deliver standardized services. Connections are always initiated from the Consistacom end, and data is always extracted in a read-only fashion.

The data visible to Consistacom is limited to Avaya administration details, via a standard Avaya administration interfaces. This limits Consistacom's vision to the telephone numbers and names within your organization. It does not expose any customer data such as name, Social Security Number, customer account number, or digits dialed by a customer when interacting with the Avaya system, nor does it provide access to your other IT systems. Once collected, the Avaya data is processed by Consistacom, retained for a short time consistent with the service provided, and then destroyed.

There are three Internet Standard ways of establishing secure connections between Consistacom and the End User: a) a Secure Shell connection, b) a site-to-site Virtual Private Network (VPN), and c) a SSL VPN.

### **The SSH Option:**

- Has few "moving parts" to configure and maintain in the customer's data network, but some configuration is required
- Provides encryption end to end, including login IDs and passwords
- Provides one level of authentication, at the Avaya Communication Manager switch
- Is available for Avaya Communication Manager 3.0 and above

### **The Site-To-Site VPN Option:**

- Implements site-to-site private networks across the public Internet
- Provides full compatibility and flexibility within the IPsec VPN standard
- Requires negotiation of the VPN configuration between Consistacom and End User
- Requires more Data Network team involvement than SSH
- Only encrypts data between VPN Peers, not end to end
- Provides two levels of authentication: 1) between VPN peer devices, 2) at the Avaya Communication Manager switch
- Is available for Definity 9.5 and above, including all MultiVantage and Communication Manager versions

### **The SSL-VPN Option**

- Is become ubiquitous in corporate data networks, so it is usually readily available
- Requires the least data network configuration of the three options
- Is only suitable for short-term connections, such as those used for one-time or infrequent deliveries of Vector Vision Services

Consistacom favors the SSL-VPN approach for one-time deliveries. Most corporations have a standard process for approving and provisioning these connections, leading to faster delivery dates for your Vector Vision services. If a long-term connection is required, Consistacom recommends the SSH approach. It does not eliminate the need for corporate data networking involvement, but reduces the resources needed from that group. It also eliminates the brief VPN setup delay for change control on the Consistacom end.

*A secure connection technology comparison chart is on the reverse side*



Comparison of Secure Network Connection Options  
Remotely Hosted PBX Management Services  
Provided by Consistacom

Setup Requirements	SSH		SSL-VPN		Site To Site VPN	
	Voice	Data	Voice	Data	Voice	Data
Assign a public IP address for PBX		D				D
Open SSH port 5022 on CM	V*		V*		V*	
Open SSH port 5022 on firewall, limited to connections from Consistacom to PBX's public IP		D		Possibly		Possibly
Negotiate site to site VPN configuration					V	D
Configure and test VPN connectivity						D
Data Network Change Management review and delay		?				D
Assign unique CM login ID and password	V		V		V	
Benefits	SSH		SSL-VPN		Site To Site VPN	
Can connect to CLAN Media Server		✓		✓ ✓		✓ ✓
Encryption	End To End		Outside your firewall		Between Firewalls	
OK for short term connections	✓		✓		✓	
OK for persistent connections	✓				✓	

V\* indicates you should check whether SSH is already enabled on your Communication Manager system. SSH is available on CM versions 3.0 and above. Avaya interfaces used by Vector Vision Technology require the use of SSH with CM versions 4.0 and above.