TENERÓS™

Building A Secure Microsoft® Exchange Continuity Appliance

Teneros, Inc.
215 Castro Street, 3rd Floor
Mountain View, California
94041-1203 USA

p 650.641.7400
f 650.641.7401
www.teneros.com

ALWAYS
ON AVAILABLE ACCESSIBLE

Building A Secure Microsoft® Exchange Continuity Appliance

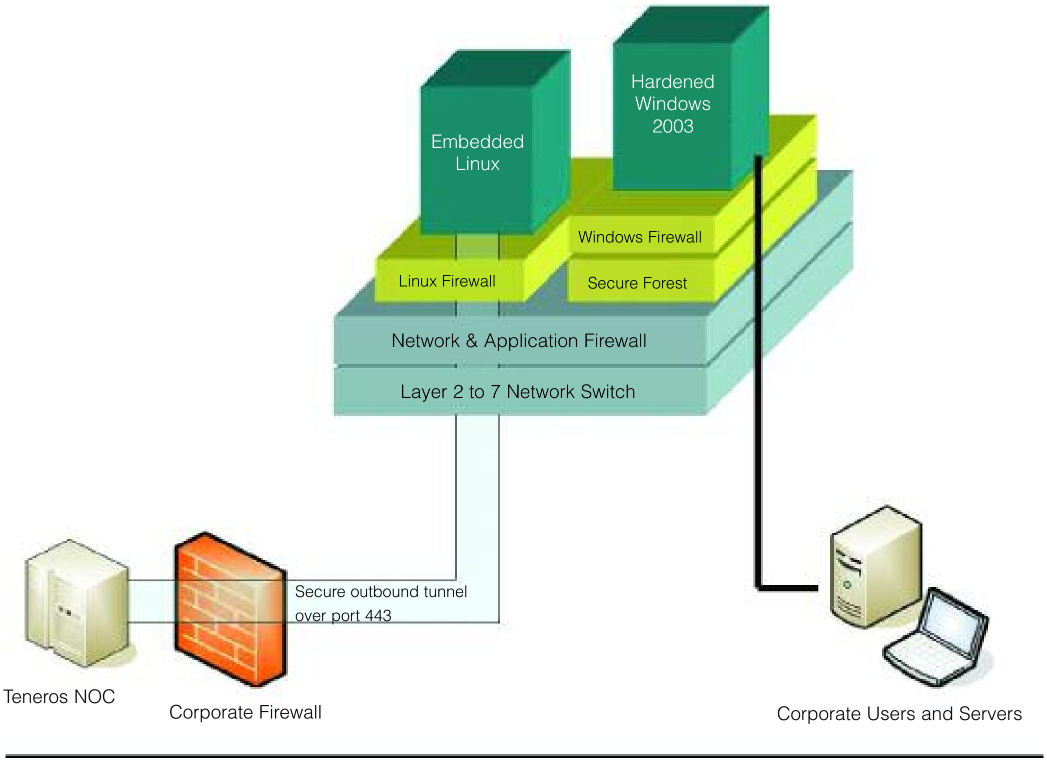
Introduction

A comprehensive security strategy comprises three key elements: preventing security lapses, protecting against security attacks, and limiting the damage in the event of a security breach. The Teneros Application Continuity Appliance™ (ACA) for Microsoft® Exchange has been architected with these three elements in mind. This paper discusses the security architecture of the ACA and how it supports a company's security strategy.

Network topology overview

The ACA sits inline with the Exchange backend server. It is connected between the network switch and the Exchange backend server. In addition, the ACA is in the same subnet as the Exchange backend server. During failover, the ACA assumes the network identity (including the IP address) of the Exchange server.

ACA Security Infrastructure


Hardened Windows 2003
Embedded Linux
Windows Firewall
Linux Firewall
Secure Forest
Network & Application Firewall
Layer 2 to 7 Network Switch
Secure outbound tunnel over port 443
Teneros NOC
Corporate Firewall
Corporate Users and Servers

Teneros Application Continuity Appliance security objectives

➲Prevention

- **Multiple layers of defense:** The built-in security architecture of the ACA must protect it from a single point of security failure i.e. the ACA must have the ability to recover from a security breach because it has multiple independent security sub-systems in place.
- **Secure NOC communication:** No access can be allowed to the customer email data from the Teneros Network Operations Center (NOC). Furthermore, all communication between the ACA and the NOC must be secure from eavesdropping. Lastly, the methodology used by the ACA to connect to the NOC must be compliant and inter-operable with the corporate security infrastructure.
- **Security patches:** The ACA should automatically remain up-to-date with the latest software security fixes and patches.

➲Protection

- **Defend intrusion attacks from the internet:** Malicious attacks on the ACA from the internet should be successfully defended.
- **Defend intrusion attacks from the corporate network:** Malicious attacks on the ACA from within the corporate network should be successfully defended.
- **Defend email based virus attacks:** The ACA should eliminate email based virus attacks. When serving users as well as in the standby mode, the ACA should detect emails containing viruses and quarantine them.

➲Control of a Security Breach

- In the unlikely event of a security breach, the ACA should have the ability to disengage from the customer network without causing damage.

➲Prevention

Multiple layers of defense

Many security solutions suffer from an architectural flaw; they execute on the same system which they are trying to secure. As a result, if the system is compromised, the security solution can be compromised or worse, disabled. In order to provide multiple, independent layers of security, the ACA is designed with a multi-subsystem security architecture, referred to as the Secure Appliance Framework (SAF). The SAF has three independent subsystems that enforce security at different levels as well as monitoring each other for security compromise. All three subsystems are isolated from each other such that a security violation on one system does not compromise another system.

- **Windows subsystem:** The Windows subsystem is running a hardened version of the Microsoft Windows 2003 server. The built-in Windows firewall protects the server from network port based attacks. By shutting down network services that are not needed by the ACA, the Windows subsystem gets further secured.
- **Linux subsystem:** The Linux subsystem runs a carrier-grade version of Linux on proprietary hardware. This hardened version of Linux is used widely in military equipment and is known for its security and reliability. Only the bare minimum network ports are open on this subsystem and there is an active network firewall detecting network based attacks. The Linux subsystem also has the ability to inspect and filter all network traffic being directed to the Windows subsystem. This provides an additional layer of protection for the Windows subsystem.
- **Switch subsystem:** The outermost layer of security in the ACA is Teneros' proprietary layer 3 through layer 7 embedded network switch. This switch partitions and restricts the network access to both the Windows and the Linux subsystems based on a set of pre-defined network rules and firewall settings. Furthermore, the switch is capable of restricting

harmful traffic at the network level, before it reaches the application.

Secure NOC communication

- **Encryption:** All communication between the ACA and the Teneros NOC is encrypted and secured using 128 bit SSL encryption as well as digital certificate protection. Each ACA must prove its unique identity to the NOC before it can create a two way network connection with the NOC. Once the secure connection is established, the ACA utilizes the built-in SSL certificates to encrypt the ongoing network traffic.
- **Interoperability with Enterprise Firewall:** The ACA to NOC communications have been designed to comply with the enterprise security guidelines and the firewall settings. The ACA creates an outbound connection over port 443 (SSL outbound port) to the NOC. In general, this does not require modifications of existing security settings in the enterprise firewall. The ACA communicates via both, the SSH and the SSL protocols with the Teneros NOC.
- **Access to corporate data:** The ACA has been architected to provide privacy for the customer email data. The customer email data is only accessible to the application running on the Windows subsystem (such as Microsoft Exchange). All communication with the Teneros NOC is handled by the Linux subsystem. Both of these subsystems are isolated in both the software and the hardware. Their interaction is limited to the standard API calls implemented by Teneros. As a result, the Linux subsystem has no ability to access the customer email data. All patches, security fixes, and antivirus updates are downloaded by the Linux subsystem from the NOC and securely handed over to the Windows subsystem for the application.
- **Human access to the ACA:** The ACA only allows network connections via a pull model. The ACA initiates all connections to the NOC. Once a connection is formed, any attempts to connect to the ACA via human interaction based protocols such as telnet, ftp or remote desktop is blocked by the network firewall rules. This assures that no human access is possible to the ACA from the NOC. All operational "health" updates are sent to the NOC programmatically by the ACA.
- **Monitoring of network traffic:** In the event that a customer wants to monitor the communications between their ACA and the Teneros NOC to verify Teneros claims, the ACA architecture allows for this option. Use of this optional feature requires implementing an Intercept server with Teneros professional services. The Intercept server forms a two way proxy between the ACA and the NOC. The communication channel between the Intercept server and the NOC is encrypted and secure. However the communication channel between the ACA and the Intercept server, which is placed on the customer LAN, is unencrypted. Hence, the network communication between the ACA and the NOC can be monitored by tapping on this channel.
- **Private NOC:** The ACA architecture allows large customers to deploy a private network operations center which sits between the customer network and the Teneros NOC. This allows elimination of all direct communication between the ACA and the Teneros NOC.

Security patches

- **Automated maintenance from the NOC:** A critical element of security is remaining current with the latest security fixes and patches. The ACA automatically receives the latest updates and patches from the Teneros NOC. This update and patch protection ensures that the security vulnerabilities are eliminated from the ACA before they can be exploited by hackers.

➲Protection

Defend intrusion attacks from the internet

- **Corporate firewall:** The ACA is located behind and protected by the corporate firewall. All existing firewall rules and settings are automatically applied to the ACA as all of the ACA communication traffic passes through the corporate firewall. Therefore, the ACA is protected from most malicious attacks assuring that the ACA is at least as safe as the rest of the network.
- **Built-in firewall:** The three subsystems within the ACA: Windows, Linux and the Switch have in-built network firewalls to eliminate malicious attacks from the internet that have penetrated the corporate firewall. The firewall rules for these subsystems are continuously updated on

the ACA from the NOC. Furthermore if one of the subsystems were to be infected, the other subsystems have the ability to detect and quarantine the infected subsystem at the network level, until it is repaired through the NOC. Since all three subsystems are running separate operating systems with separate hardware, the likelihood of more than one subsystem getting simultaneously compromised is remote.

Defend against intrusion attacks from the corporate network

- **Access privilege lock-down:** Security breaches can also occur from within the corporate network through an infected laptop or mobile device. Such attacks usually cannot be blocked by the corporate firewall. Furthermore such attacks can utilize the credentials of the employee owning the laptop, to gain access to other machines. This can also happen if one of the servers (such as the Exchange or the MSSQL server) gets compromised through the internet and starts spreading the attack to other peer servers. In such scenarios most of the enterprise servers are vulnerable as the malicious code gets executed with valid credentials that give it permission to access other servers. The ACA is protected from such internal attacks because it resides in an isolated directory forest. Users in the corporate forest have no special privileges on the ACA since the ACA is not a part of the corporate directory forest.

Defend against email based virus attacks

- **Sophos:** The ACA has built-in protection from email based virus attacks. Email virus detection software from Sophos is integrated in the ACA. The latest virus signatures are continuously downloaded from the Teneros NOC, keeping the ACA up to date. Upon detection of an infected email, the Sophos software quarantines the email.

➲Control of a Security Breach

The ACA has the unique ability to disengage from the customer network in the unlikely event of a security breach or system failure that is not defended by the ACA security infrastructure. The internal switch subsystem can instantly cutoff the ACA from the network and the ACA becomes an Ethernet wire.